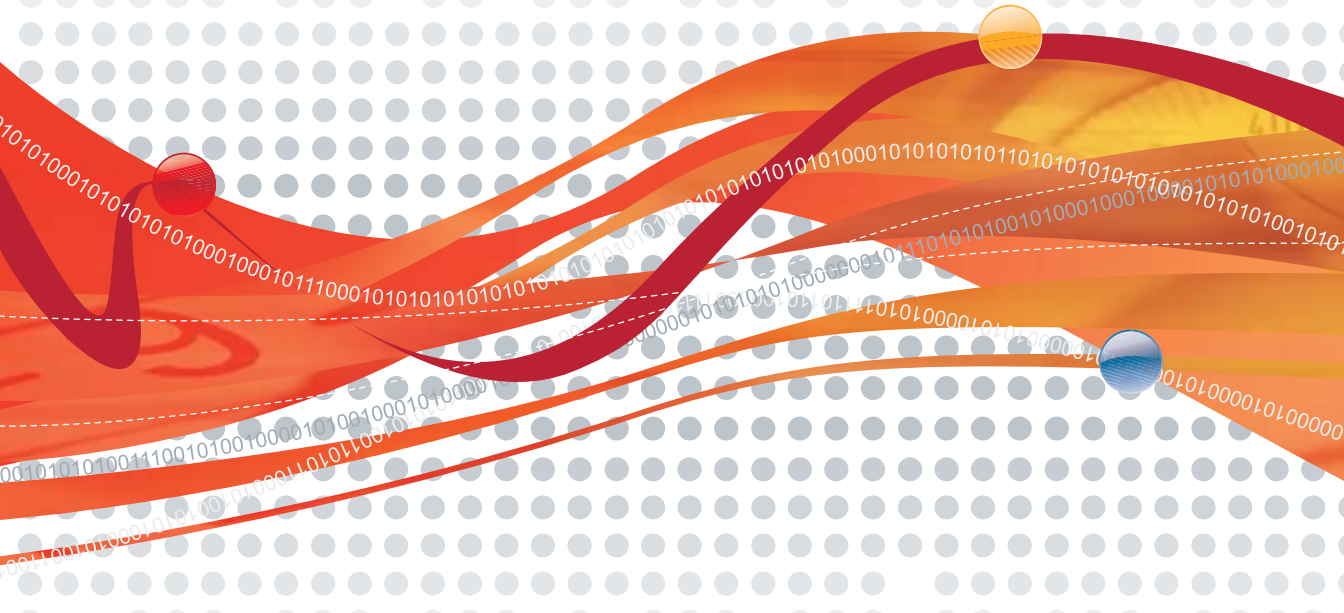
TREND MICRO™

InterScan™ Messaging Security Suite 7

Comprehensive threat protection at the Internet messaging gateway

for LINUX™ & Solaris™

Administrator's Guide



Messaging Security

Document Part Number: MSEM73220/70515

Release Date: September 2007

The Administrator's Guide for Trend Micro InterScan Messaging Security Suite 7.0 (IMSS) is intended to provide you with instructions on how to configure and administer IMSS to ensure that your network is well-protected against various malware. You should read through this document after installing IMSS. For instructions on deploying and installing IMSS, please refer to the IMSS Installation Guide.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

InterScan Messaging Security Suite 7.0 Documentation vi
Audience vi
Document Conventions vii

Chapter 1: Getting Started

Opening the IMSS Web Management Console 1-2
Using the Online Help 1-2
Viewing the Web Management Console Using Secure Socket Layer 1-3
Creating an SSL certificate 1-3
Performing Basic Configuration with the Configuration Wizard 1-4
Accessing the Configuration Wizard 1-4
Step 1: Configuring the Notification Settings 1-5
Step 2: Configuring the Update Source 1-6
Step 3: Configuring the LDAP Settings 1-7
Step 4: Configuring Internal Addresses 1-9
Step 5: Configuring Control Manager Server Settings 1-10
Step 6: Configuring Product Settings 1-11
Step 7: Verifying Settings Summary 1-11
IMSS Services 1-12
Starting or Stopping Services 1-13
Opening the End-User Quarantine Console 1-14
Log On Name Format 1-14

Chapter 2: Configuring IMSS Settings

IP Filtering Service 2-2
Using Network Reputation Services 2-2
Using the SPS Activation Code 2-2
Preparing Your Message Transfer Agent for use with Network Reputation Services 2-3
Using the NRS Management Console 2-4
Configuring IP Filtering 2-5

Step 1: Enable NRS and IP Profiler 2-5
Step 2: Enable IP Profiler Rules 2-6
Step 3: Configure NRS 2-7
Step 4: Add IP Addresses to the Approved List 2-8
Step 5: Add IP Addresses to the Blocked List 2-9
Querying IP Filtering Logs 2-11
Scanning SMTP Messages 2-12
Enabling SMTP Connections 2-12
Configuring SMTP Routing 2-13
Configuring SMTP Settings 2-14
Configuring Connections Settings 2-14
Configuring Message Rule Settings 2-16
Configuring Domain-based Delivery Settings 2-17
Scanning POP3 Messages 2-19
Understanding POP3 Scanning 2-19
Requirements 2-20
Enabling POP3 Scanning 2-20
Configuring POP3 Settings 2-21
Managing Policies 2-23
How the Policy Manager Works 2-23
Understanding Address Groups 2-25
Managing Address Groups 2-26
Adding an Address Group 2-26
Editing or Deleting an Address Group 2-28
Searching for an LDAP user or group 2-30
Configuring Internal Addresses 2-32
Adding Policies 2-34
Specifying a Route 2-34
Specifying Scanning Conditions 2-36
Specifying Actions 2-40
Specifying Priority 2-43
Example 1 2-45
Example 2 2-49
Using the Asterisk Wildcard 2-53
Updating Scan Engine and Pattern Files 2-55
Specifying an Update Source 2-55
Performing a Manual Update 2-56

Rolling Back a Component Update 2-57
Configuring Scheduled Update 2-57
Configuring Log Settings 2-59

Chapter 3: Backing Up, Restoring, and Replicating Settings

Backing Up IMSS 3-2
Restoring IMSS 3-4
Replicating Settings 3-5
Enabling Control Manager Agent 3-5
Replicating Settings from Control Manager 3-6

Chapter 4: Maintaining IMSS

Monitoring Your Network 4-2
Viewing Statistics 4-2
Interpreting the Statistics 4-3
Performance Overview 4-4
Scan Performance 4-5
IP Filtering Performance 4-6
Generating Reports 4-7
Types of Report Content 4-7
Adding One-time Reports 4-8
Configuring Scheduled Reports 4-10
Logs 4-14
Querying Logs 4-14
Quarantine and Archive 4-16
Configuring Quarantine and Archive Settings 4-16
Querying Quarantined and Archived Messages 4-18
Configuring User Quarantine Access 4-20
Adding/Removing an EUQ Database 4-21
Adding an EUQ Database 4-21
Removing an EUQ Database 4-23
Command-line options for euqtrans tool 4-23
Event Notifications 4-24
Configuring Delivery Settings 4-25
Configuring Event Criteria and Notification Message 4-26
Managing Administrator Accounts 4-29
Adding Administrator Accounts 4-29

Editing or Deleting Administrator Accounts 4-30
Configuring Scanner and Policy Connections 4-32

Chapter 5: Troubleshooting, FAQ, and Support

Troubleshooting 5-2
Frequently Asked Questions 5-9
Postfix MTA Settings 5-9
IMSS Components 5-9
Network Reputation Services 5-11
IP Profiler 5-12
Quarantine and Archive 5-16
End-User Quarantine 5-16
Spam Protection Service 5-18
ActiveUpdate 5-19
Others 5-19
Using the Knowledge Base 5-24
Contacting Support 5-24

Appendix A: IMSS Scripts

Invoking IMSS Scripts A-2

Appendix B: Default Directory Locations

Default Mail Queues B-2
eManager, Virus and Program Logs B-3
Temporary Folder B-3
Notification Pickup Folder B-3

Index

Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Security Suite 7.0 Administrator's Guide*. This manual contains post-installation information to get InterScan Messaging Security Suite (IMSS) up and running. Please refer to the Online Help in the Web management console for detailed information on each field on the user interface.

This preface discusses the following topics:

- *InterScan Messaging Security Suite 7.0 Documentation* on page vi
- *Audience* on page vi
- *Document Conventions* on page vii

InterScan Messaging Security Suite 7.0 Documentation

The InterScan Messaging Security Suite 7.0 (IMSS) documentation consists of the following:

- **Installation Guide**—Contains introductions to IMSS features, system requirements and provides instructions on how to deploy and upgrade IMSS in various network environment.
- **Administrator's Guide**—Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.
- **Online Help**—Provides detailed instructions on each field and how to configure all features through the user interface. To access the online help, open the Web management console, then click the help icon ( ).
- **Readme Files**—Contain late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The *Installation Guide, Administrator's Guide* and *readme files* are available at http://www.trendmicro.com/download.

Audience

The InterScan Messaging Security Suite documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP and POP3 protocols
- Message transfer agents (MTAs), such as Postfix
- LDAP
- Database management

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

Document Conventions

To help you locate and interpret information easily, the IMSS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and other user interface items
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that must be avoided

Chapter 1

Getting Started

This chapter explains how to logon to the Web management console and provides instructions on what to do immediately after installation to get IMSS 7.0 up and running.

Topics include:

- *Opening the IMSS Web Management Console* on page 1-2
- *Viewing the Web Management Console Using Secure Socket Layer* on page 1-3
- *Performing Basic Configuration with the Configuration Wizard* on page 1-4
- *IMSS Services* on page 1-12
- *Opening the End-User Quarantine Console* on page 1-14

Opening the IMSS Web Management Console

You can view the IMSS management console with a Web browser from the server where you installed the program, or you can view the management console remotely across the network.

To view the console in a browser, go to the following URL:

- https://<target server IP address>:8445

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

The default logon credentials are as follows:

- Administrator user name: **admin**
- Password: **imss7.0**

Type the log on credentials the first time you open the management console and click the **Enter** button.

Note: If you are using Internet Explorer (IE) 7.0 to access the Web management console, IE will block the access and display a popup dialog box indicating that the certificate was issued from a different Web address. Simply ignore this message and click **Continue to this Web site** to proceed.

Tip: To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.

Using the Online Help

The IMSS Web management console comes with an Online Help that provides a description of each field on the user interface.

To access page-specific Online Help from the IMSS Web management console, click the Help icon located at the top right corner of the page.

To access the *table of contents* for the Online Help, click the Help icon next to the **Log Off** hyperlink on the right of the page header.

Viewing the Web Management Console Using Secure Socket Layer

The IMSS Web management console supports encrypted communication, using SSL. After installing IMSS, SSL communication should work because the installation contains a default certificate. Trend Micro suggests creating your own certificate to increase security.

If you want to use your own certificate, replace the following:

```
$IMSS_HOME/UI/tomcat/sslkey/.keystore
```

Creating an SSL certificate

Do the following:

1. Create the Tomcat SSL certificate as follows:

   ```
   keytool -genkey -alias tomcat -keyalg RSA  -keystore
   /opt/trend/imss/UI/tomcat/sslkey/.keystore
   ```

   For more details on SSL configuration in Tomcat, please visit:

   http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

2. Create the Apache SSL certificate as follows:

   a. Generate a Private Key and Certificate Signing Request (CSR)

   ```
   openssl req -new > new.cert.csr
   ```

   b. Remove pass-phrase from the key

   ```
   openssl rsa -in privkey.pem -out new.cert.key
   ```

   c. Generate a Self-Signed Certificate

   ```
   openssl x509 -in new.cert.csr -out new.cert.cert -req
   -signkey new.cert.key -days 1825
   ```

   d. Copy the certificate and key to the Apache path

   ```
   cp new.cert.cert
   $IMSS_HOME/UI/apache/conf/ssl.crt/server.crt
   cp new.cert.key
   $IMSS_HOME/UI/apache/conf/ssl.key/server.key
   ```

Performing Basic Configuration with the Configuration Wizard

IMSS provides a configuration wizard to help you configure the basic settings required to get IMSS up and running.

The configuration wizard guides you through seven (7) steps of configuring the following settings:

Step 1: Notification settings

Step 2: Update source

Step 3: LDAP settings

Step 4: Internal addresses

Step 5: Control Manager server settings

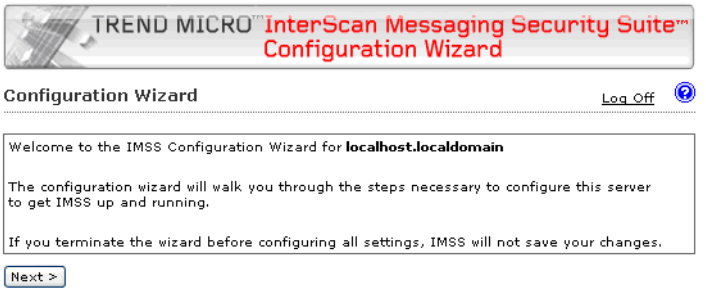
Step 6: Product settings

Step 7: Settings summary

Accessing the Configuration Wizard

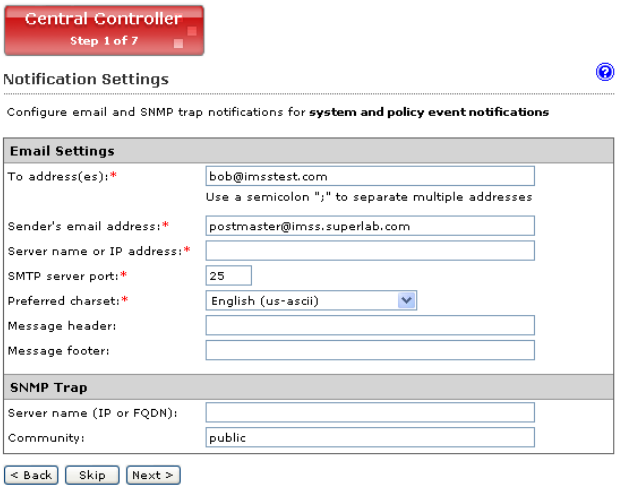
Access the wizard using one of the following methods:

- Log on to the Web management console and make sure the **Open Configuration Wizard** is selected on the log on screen, and then log on. The wizard opens.
- If you are already logged on to the Web management console, choose **Administration > IMSS Configuration > Configuration Wizard**. The wizard opens in a new window.



Step 1: Configuring the Notification Settings

1. After you read the welcome screen, click **Next**. The **Notification Settings** screen appears.

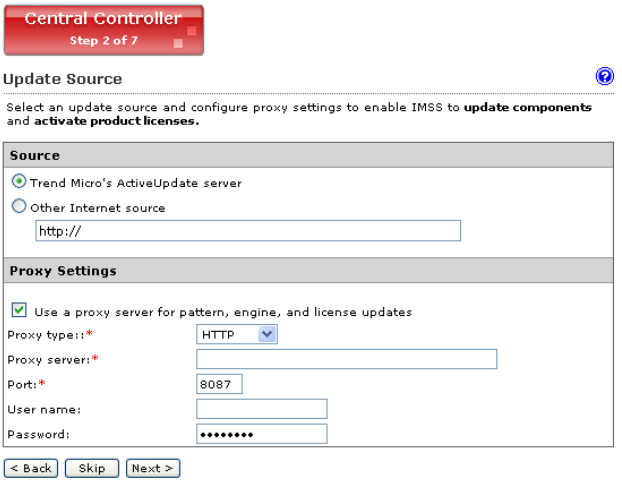


2. Configure the following notification settings, which IMSS will use for all default system and policy event notifications:
   - **Email Settings**—Type the sender and receiver addresses, the name of the server that IMSS delivers mail to, the SMTP server port, the language character set, and any additional headers or footers to add to the message.

- **SNMP Trap**—If you have an SNMP server on your network, type the server name and the community name.

Step 2: Configuring the Update Source

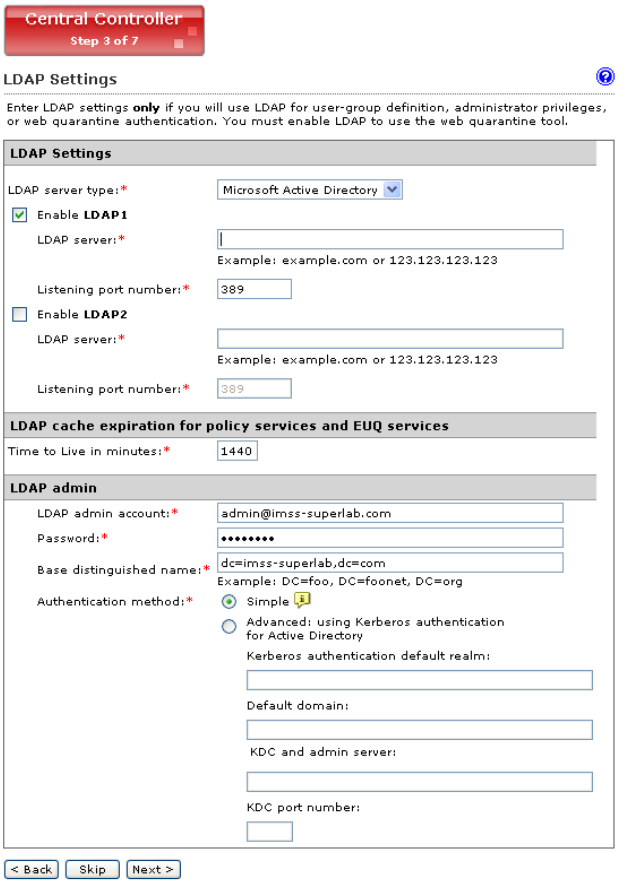
1. Click **Next**. The **Update Source** screen appears.



2. Configure the following update settings, which will determine from where IMSS will receive its component updates and through which proxy (if any) IMSS needs to connect to access the Internet:
   - **Source**—Click **Trend Micro ActiveUpdate (AU) server** to receive updates directly from Trend Micro. Alternatively, click **Other Internet source** and type the URL of the update source that will check the Trend Micro AU server for updates. You can specify an update source of your choice or type the URL of your Control Manager server, if applicable.
   - **Proxy Settings**—Select the **Use proxy server** check box and configure the proxy type, server name, port, user name, and passwords.

Step 3: Configuring the LDAP Settings

1. Click **Next**. The **LDAP Settings** screen appears.



2. Do the following to enable LDAP settings:
   a. Next to **LDAP server type**, select one of the following:
      - **Microsoft Active Directory**
      - **Domino**

- **Sun iPlanet Directory**

b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.

c. Type the names of the LDAP servers and the port numbers they listen on.

d. Under **LDAP Cache Expiration for Policy Services and EUQ services**, type a number that represents the time to live next to the **TTL in minutes** field.

e. Under **LDAP Admin**, type the administrator account, its corresponding password, and the base-distinguished name. See Table 1-1 for a guide on what to specify for the LDAP admin settings.

LDAP Server	LDAP Admin Account (examples)	Base Distinguished Name (examples)	Authentication Method
Active Directory	• Without Kerberos: user1@imsstest.com (UPN) or imsstest\user1 • With Kerberos: user1@imsstest.com	dc=imsstest, dc=com	• Simple • Advanced (with Kerberos)
Domino	user1/imsstest	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=imsstest, dc=com	dc=imsstest, dc=com	Simple

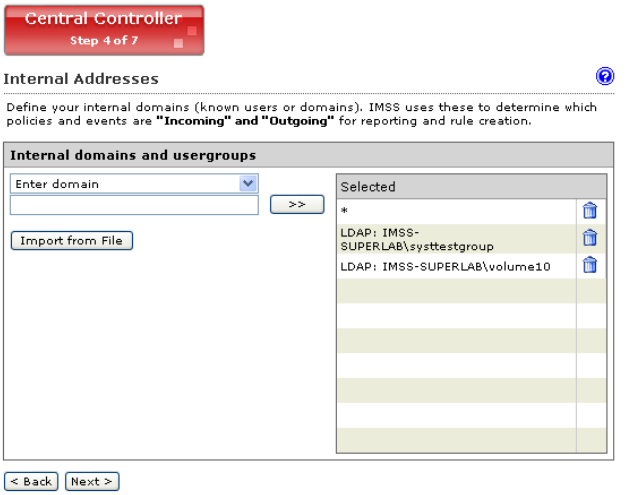
TABLE 1-1. LDAP admin settings

f. Next to **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.

Note: Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication. You must enable LDAP to use End-User Quarantine.

Step 4: Configuring Internal Addresses

1. Click **Next**. The **Internal Addresses** screen appears.

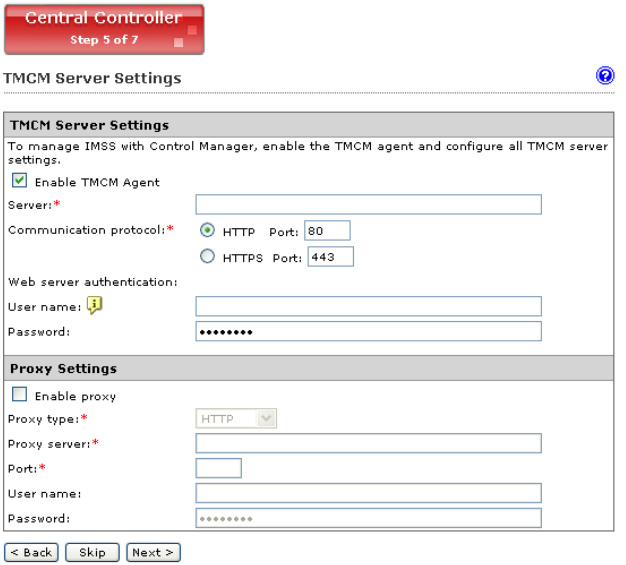


2. IMSS uses the internal addresses to determine whether a policy or an event is inbound or outbound.
   - If you are configuring a rule for outgoing messages, the internal address list applies to the senders.
   - If you are configuring a rule for incoming messages, the internal address list applies to the recipients.

   To define internal domains and usergroups, do one of the following:
   - Select **Enter domain** from the drop-down list, type the domain in the text box, and then click >>.
   - Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Type an LDAP group name for which you want to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click >>.

Step 5: Configuring Control Manager Server Settings

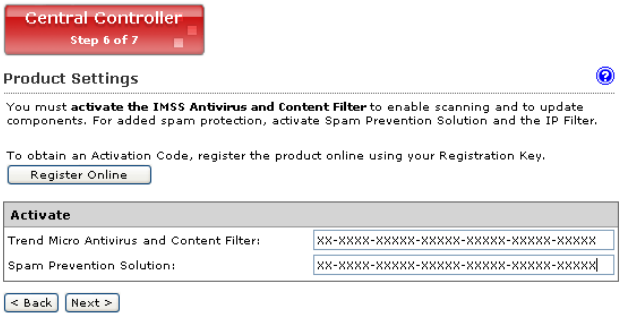
1. Click **Next**. The **TMCM Server Settings** screen appears.



2. If you will use Control Manager to manage IMSS, do the following:
   a. Select **Enable TMCM Agent** (installed with IMSS by default).
   b. Next to **Server**, type the TMCM IP address or FQDN.
   c. Next to **Communication protocol**, select **HTTP** or **HTTPS** and type the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.
   d. Under **Web server authentication**, type the user name and password for the Web server if it requires authentication.
   e. If a proxy server is between IMSS and TMCM, select **Enable proxy**.
   f. Type the proxy server port number, user name, and password.

Step 6: Configuring Product Settings

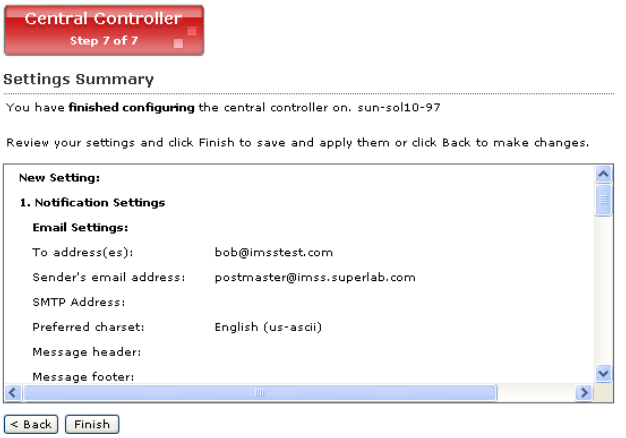
1. Click **Next**. The **Product Settings** screen appears. You must activate the Antivirus and Content Filter to enable scanning and security updates. To obtain an Activation Code, register the product online using the supplied Registration Key.



2. Type the Activation Codes for the products you want to activate. If you do not have an Activation Code, click **Register Online** and follow the directions at the Trend Micro Registration Web site.

Step 7: Verifying Settings Summary

1. Click **Next**. A **Summary** screen appears.



2. If your settings are correct, click **Finish**.

   To modify any of your settings, click **Back** and keep moving through the screens until your settings are complete.

IMSS Services

The scanner and policy services must be started in order to start protecting your network using IMSS. You can however, choose whether to install or start the EUQ service.

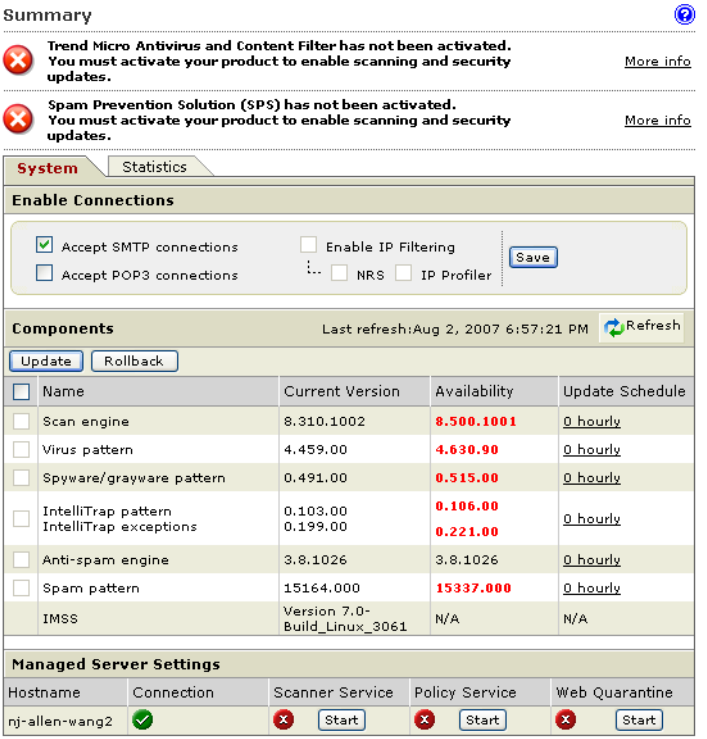
- **Scanner Services**—Performs scanning of SMTP/POP3 traffic.
- **Policy Services**—Acts as a remote store of rules for the scanner services to enhance rule lookups.
- **EUQ Services**—Hosts a Web-based console to enable end-users to view, delete and release spam messages addressed to them.

For more information on these services, refer to the IMSS Installation Guide.

Starting or Stopping Services

After you have successfully installed IMSS and configured the various settings, you have to start the services to begin scanning for malware and other threats. Likewise, you may need to stop IMSS services prior to performing an upgrade or backup function.

1. Choose **Summary** from the menu. The Summary screen appears with the default System tab selected.



2. Under the Managed Server Settings section, click the **Start** or **Stop** buttons for the service(s) that you would like to start or stop.

Opening the End-User Quarantine Console

Before you can access the EUQ Web console, ensure that you have done the following:

1. Configured the LDAP settings. See *Step 3: Configuring the LDAP Settings* on page 1-7.
2. Enabled User Quarantine Access. See *Configuring User Quarantine Access* on page 4-20.

You can view the EUQ Web console from the computer where the program was installed or you can view the EUQ Web console remotely across the network.

To view the console from another computer on the network, go to:

- Primary EUQ service—`https://<target server IP address>:8447`
- Secondary EUQ service—`https://<target server IP address>:8446`

WARNING! *To successfully access all Web consoles on secondary EUQ services, you must synchronize the system time of all EUQ services on your network.*

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Log On Name Format

The format of the user log on name for accessing the EUQ Web console differs according to the LDAP server type you have selected when configuring LDAP settings. Following are some examples of the log on name format for the three (3) types of supported LDAP servers:

- **Microsoft Active Directory**
  - Without Kerberos—`user1@imsstest.com (UPN) or imsstest\user1`
  - With Kerberos—`user1@imsstest.com`
- **Domino**—`user1/imsstest`
- **Sun iPlanet Directory**—`uid=user1, ou=people, dc=imsstest, dc=com`

Chapter 2

Configuring IMSS Settings

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSS up and running. For more details, please refer to the Online Help accessible from the Web management console.

- *IP Filtering Service* on page 2-2
- *Scanning SMTP Messages* on page 2-12
- *Scanning POP3 Messages* on page 2-19
- *Managing Policies* on page 2-23
- *Updating Scan Engine and Pattern Files* on page 2-55
- *Configuring Log Settings* on page 2-59

IP Filtering Service

The IP Filtering service has two individual components: Network Reputation Service and IP Profiler.

- Network Reputation Service filters spam senders at the connection layer.
- IP Profiler helps protect the mail server from attacks with smart profiles (SMTP) Intrusion Detection Service (IDS).

Tip: Trend Micro recommends deploying IP Filtering as the first line of defense in your messaging infrastructure.

Although most email messaging systems have a multi-layer structure that often includes some pre-existing IP blocking, spam filtering, and virus filtering, Trend Micro recommends completely removing other IP blocking techniques from the messaging environment. IP Filtering should act as the precursor to any application filtering you might use.

Using Network Reputation Services

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Network Reputation Services (NRS) filters spam by blocking the IP addresses stored in this database.

Using the SPS Activation Code

IP Filtering Service, which includes NRS and IP Profiler, uses the same license as Spam Prevention Solution (SPS). If you purchase the full SPS service package, you will receive a registration key that will allow you to create a customer account with Trend Micro and upon completion of the registration process, you will receive your Activation Code.

The Activation Code enables you to access the level of services according to your registration. When you activate SPS, the licensing information for IP Filtering will then appear.

For details on configuring NRS, see *Configuring IP Filtering* on page 2-5

Preparing Your Message Transfer Agent for use with Network Reputation Services

To prepare your MTA for use with NRS:

- **RBL+ Service—**Configure the MTA to reject connections that have a **550** level error code (connection refused). This error code indicates that a positive response was received from the RBL+ database. Listings in the RBL+ database are known to be spammers or sources that should not be sending email. Therefore, the standard method for handling these spammers is to reject the connections outright.

  For more information, see the following URL:

  `www.trendmicro.com/en/products/nrs/rbl/use/configure.htm`

- **Network Anti-Spam Service**—Configure your MTA to make 2 potential DNS queries, first to the QIL database and then to the RBL+ database.

  The QIL (Quick IP Lookup) database is a real-time dynamic database that contains a list of suspicious IP addresses that are sending spam. These IP addresses will be removed from the QIL database once spam stops coming from these addresses. If the QIL database does not receive a positive response, the MTA will need to make a second query to the RBL+ database, which contains a more stable list of blacklisted IP addresses.

  The MTA should temporarily deny connections that have a **450** level error code (server temporarily unavailable, please retry), when a positive response is received from the QIL database. The IP listings in this database are occasionally legitimate mail servers that may have compromised hosts behind them temporarily sending spam. If the connection request is from a legitimate mail server, it will re-queue and try sending the message at a later time. This will cause a short delay in mail delivery until the listing expires, but will not permanently block the mail.

  For more information, see the following URL:

  `www.trendmicro.com/en/products/nrs/nas/use/configure.htm`

Using the NRS Management Console

Log on to the Network Reputation Services management console to access global spam information, view reports, create or manage Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks.

This section includes basic instructions for using the NRS console. For detailed instructions on configuring the settings for each screen, see the NRS console online help. Click the help icon in the upper right corner of any help screen to access the online help.

To use the NRS Management Console:

1. Open a browser and access the following address:

   `https://nrs.nssg.trendmicro.com/`

2. Select **Global Spam Update** from the menu.
3. Click any of the following tabs:
   - **Spam Alert**—Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
   - **ISP Spam.x**—The total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISP's will change on a daily basis.
4. To view reports that summarize the query activity between your MTA and the Network Reputation Services database servers, do the following:
   a. Select **Report** from the menu.
   b. Click **Percentage queries**, **Queries per hour**, or **Queries per day**.
5. To create or manage Approved Sender IP and Blocked Sender IP lists, choose **Policy** from the menu. You can define your Approved Senders by individual IP address and CIDR by Country, or by ISP.
6. To add an ISP to the list, choose **New ISP** from the menu.

   To change your password or Activation code, choose Administration from the menu.

Configuring IP Filtering

To completely configure IP Filtering, perform the following steps:

Step 1: Enable NRS and IP Profiler

Step 2: Enable IP Profiler Rules

Step 3: Configure NRS

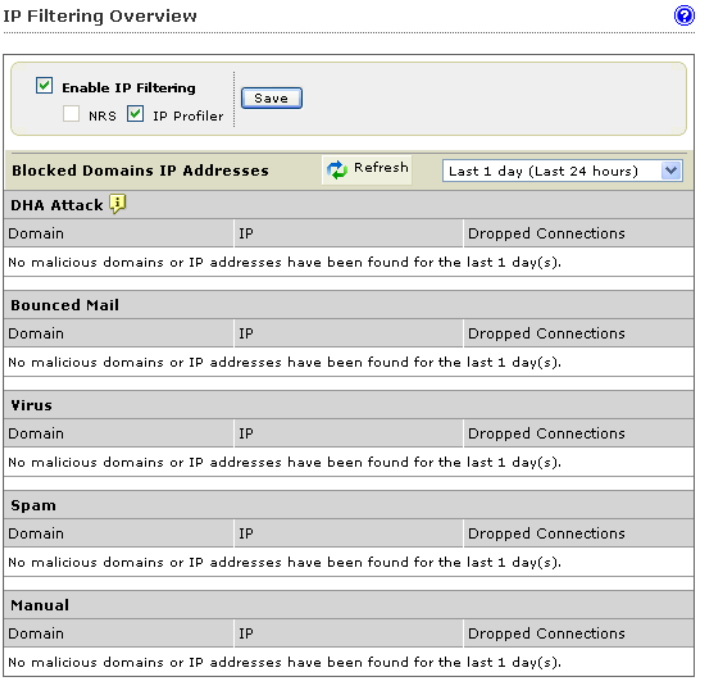
Step 4: Add IP Addresses to the Approved List

Step 5: Add IP Addresses to the Blocked List

Step 1: Enable NRS and IP Profiler

To enable NRS and IP Profiler:

1. Choose **IP Filtering > Overview** from the menu. The IP Filtering Overview screen appears.



2. Select the **Enable IP Filtering** check box. This will select both the NRS and IP Profiler check boxes.
3. Clear the **NRS** or **IP Profiler** check box, if you do not require them.
4. Click **Save**.

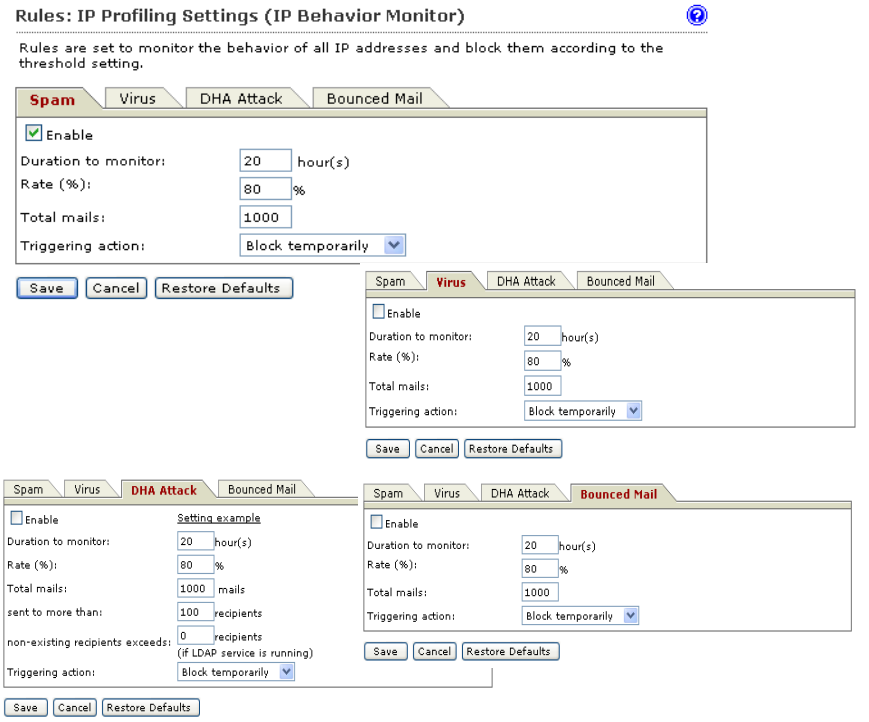
Note: If you decide to disable IP filtering subsequently, please uninstall NRS and IP Profiler manually. Disabling IP filtering from the Web management console merely unregisters IP Profiler from IMSS but does not stop NRS and IP Profiler from running. For more information on uninstalling NRS and IP Profiler, see Uninstalling Network Reputation Services and IP Profiler section of the IMSS Installation Guide.

Step 2: Enable IP Profiler Rules

IP Profiler can defend against 4 types of attacks.

To enable IP Profiler rules:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

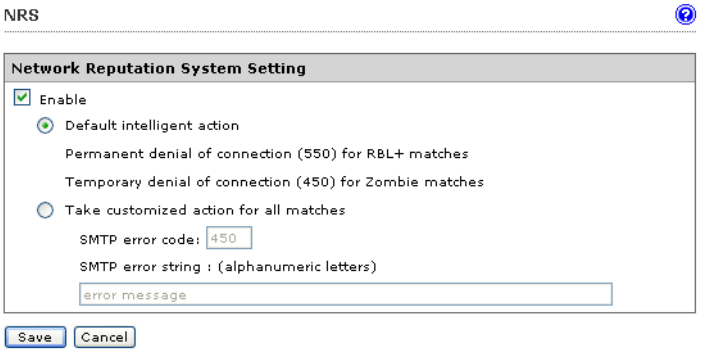


2. Select the desired tab to configure the rule settings for that threat.
3. Select the **Enable** check box.
4. Specify the required parameters (consult the online help for details).
5. Click **Save**.

Step 3: Configure NRS

To configure NRS:

1. Choose **IP Filtering > NRS** from the menu. The NRS screen appears.



2. Select the **Enable** check box.
3. Click a radio button next to one of the following:
   - **Default intelligent action**—NRS permanently denies connection (550) for RBL+ matches and temporarily denies connection (450) for Zombie matches.
   - **Take customized action for all matches**
     - **SMTP error code**—Reject any connections that have a certain SMTP code. Type an SMTP code.
     - **SMTP error string**—Type the message associated with the SMTP error code.

   Note: The above SMTP error code and error string will be sent to the upstream MTA that will then take the necessary preconfigured actions, such as record the error code and error string in a log file.

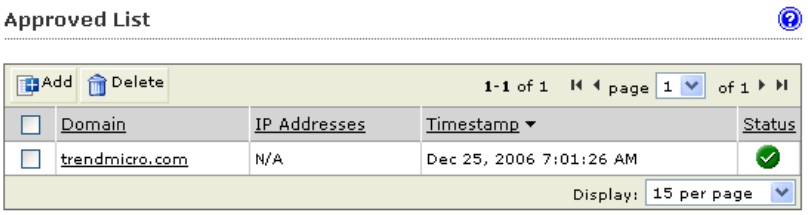
4. Click **Save**.

Step 4: Add IP Addresses to the Approved List

IMSS does not filter IP addresses or domains that appear in the Approved List.

To add an IP address to the approved list:

1. Choose **IP Filtering > Approved List** from the menu. The Approved List screen appears.



2. Click **Add**. The Add IP/Domain to Approved List screen appears.

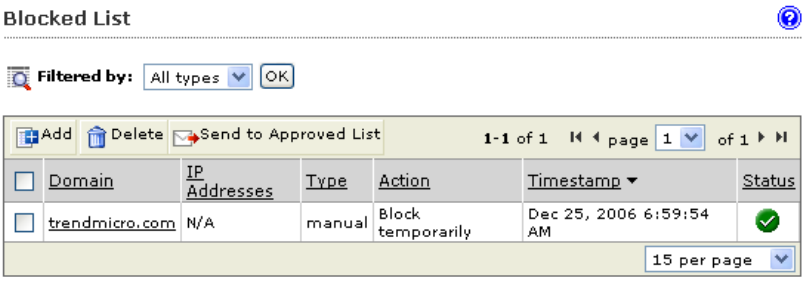
3. Select the **Enable** check box.
4. Type the domain or IP address that you would like to add to the Approved List.
5. Click **Save**. The domain or IP address appears in the Approved List.

Step 5: Add IP Addresses to the Blocked List

IMSS blocks IP addresses that appear in the Blocked List.

To add an IP address to the Blocked List:

1. Choose **IP Filtering > Blocked List** from the menu. The Blocked List screen appears.



2. Click **Add**. The Add IP/Domain to Blocked List screen appears.

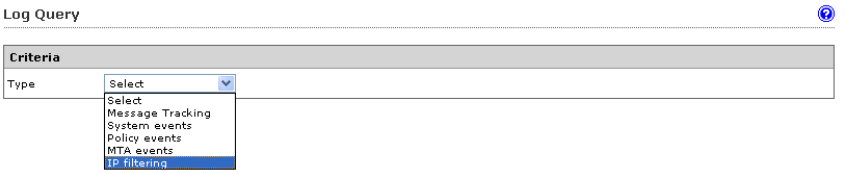
3. Select the **Enable** check box.
4. Type the domain or IP address.
5. Select **Block temporarily** or **Block permanently**.
6. Click **Save**. The domain or IP address is added to the blocked list.

Querying IP Filtering Logs

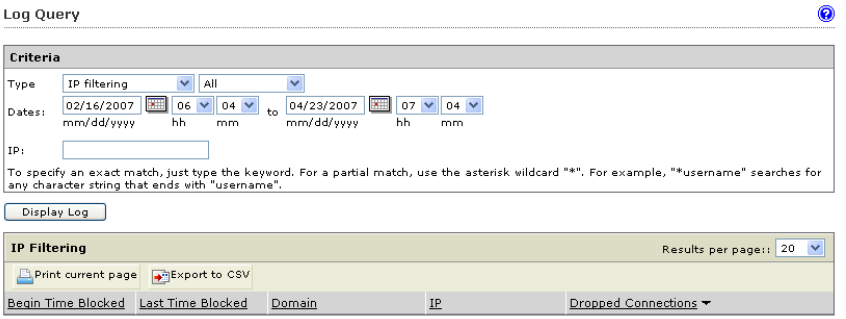
IP Filtering records events on your network as the events occur. You can query the IP Filtering action history.

To query IP filtering:

1. Choose **Logs > Query** from the menu. The Log Query screen appears.
2. For **Type** select **IP Filtering**.



3. Specify the search data (leave blank to show all data). IMSS performs an exact match by default. Separate multiple conditions with a semicolon ";".
4. Click **Display Log** to see the results.



Scanning SMTP Messages

IMSS supports three types of Message Transfer Agents (MTA). They are Postfix, Sendmail, and Qmail.

If you are using Postfix with IMSS and have deployed multiple scanner services, you can manage the SMTP routing settings for the scanner services centrally. From the IMSS Web management console, you can configure the SMTP settings and apply the same settings to all scanners.

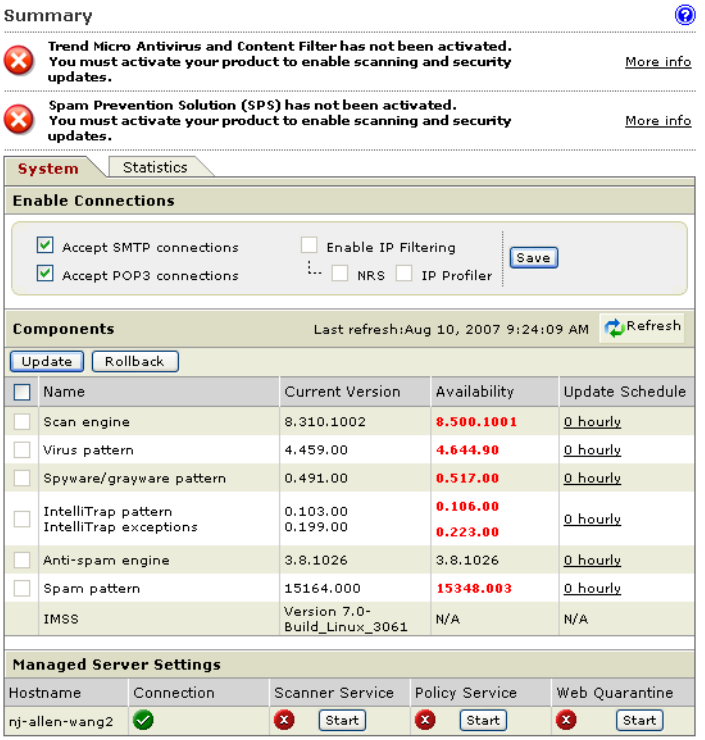
If you are using Sendmail or Qmail, you will need to manually configure the SMTP settings in the respective MTA configuration files. For details, see Preparing Message Transfer Agents section of the IMSS Installation Guide.

Enabling SMTP Connections

Before IMSS can start scanning incoming and outgoing traffic on your network, you need to enable SMTP connections.

To enable SMTP connections:

1. Choose **Summary** from the menu. The System tab appears by default.



2. Select the check box next to **Accept SMTP connections**.
3. Click **Save**.

Configuring SMTP Routing

Configuring SMTP routing involves four steps as follows:

Step 1: Configure the SMTP settings

Step 2: Configure the Connections settings

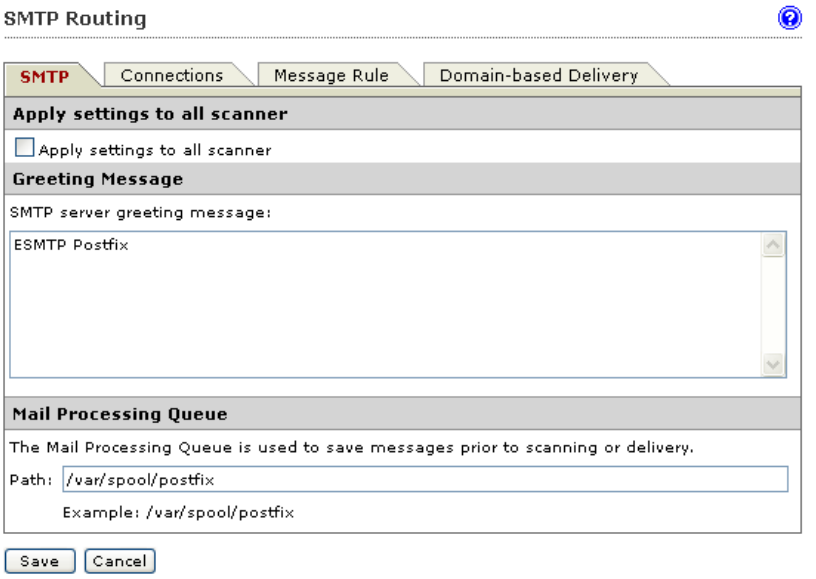
Step 3: Configure the Message Rule settings

Step 4: Configure the Domain-based Delivery settings

Configuring SMTP Settings

To specify the SMTP settings:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu. The SMTP Routing screen appears.

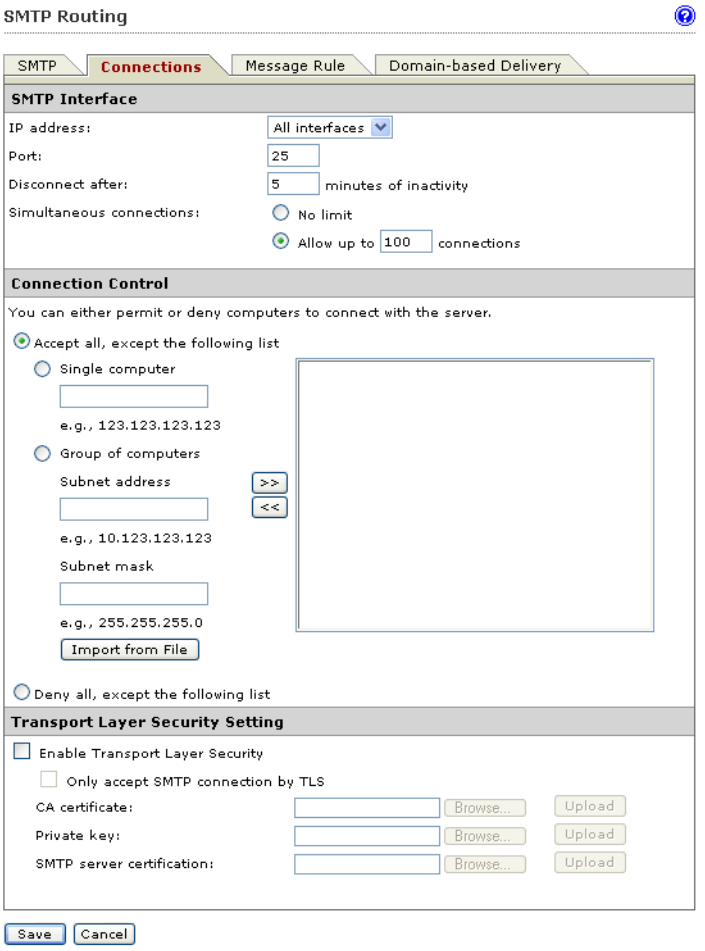


2. Select the **Apply settings to all scanner** check box.
3. Specify SMTP server **Greeting Message** (displays when a session is created).
4. Specify the **Mail Processing Queue Path**.
5. Click **Save**.

Configuring Connections Settings

To specify the Connections settings:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu**.**
2. Click the **Connections** tab. The Connections screen appears.

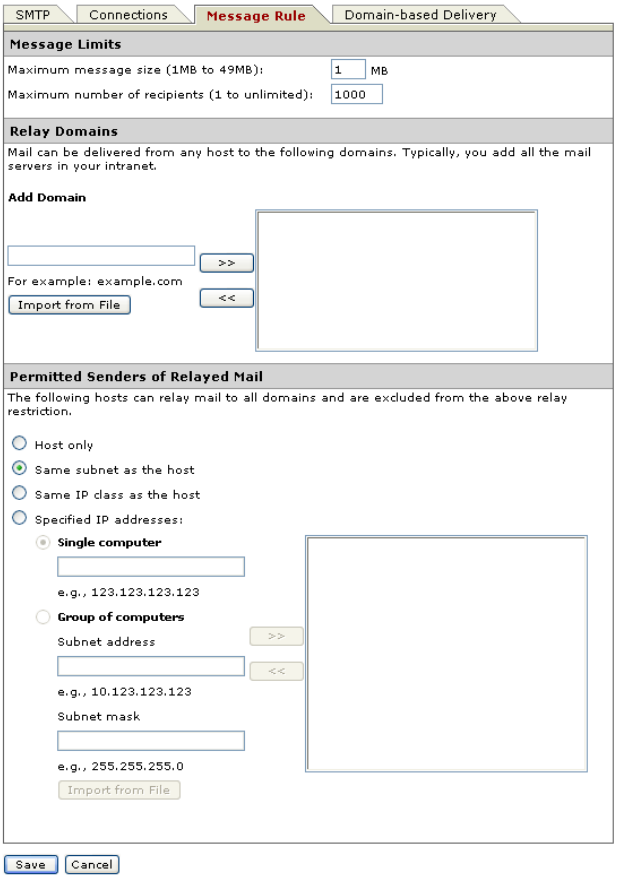


3. Specify the **SMTP Interface** and **Connection Control** parameters.
4. Specify the **Transport Layer Security Setting** parameters.
5. Click **Save**.

Configuring Message Rule Settings

To specify the Message Rules:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu.
2. Click the **Message Rule** tab. The Message Rule screen appears.



3. Specify the **Message Limits** parameters.
4. Specify the **Relay Domains**. IMSS relays the messages to the listed domains.

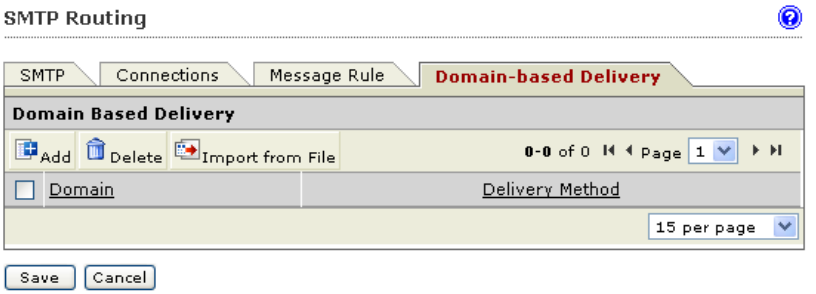
5. Specify the **Permitted Senders of Relayed Mail**.
6. Click **Save**.

Configuring Domain-based Delivery Settings

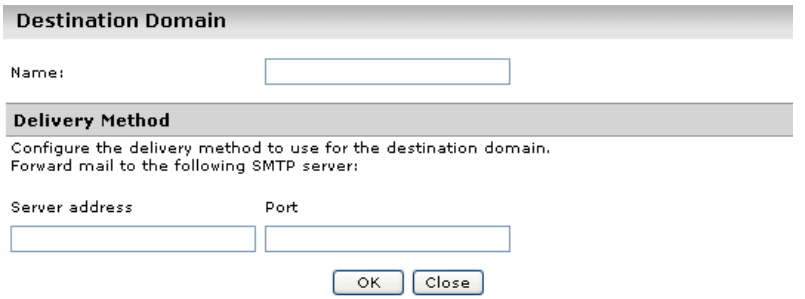
Specify settings for the next stage of delivery. IMSS finds the recipient mail domain and sends the mail to the next SMTP host for the matched domain.

To specify the Domain-based Delivery:

1. Choose **Administration > IMSS Configuration > SMTP Routing** from the menu.
2. Click the **Domain-based Delivery** tab. The Domain-based Delivery screen appears.



3. Click **Add**. The Destination Domain screen appears.



4. Specify the **Destination Domain** and **Delivery Method**.

5. Click **OK**.
6. Click **Save**.

Scanning POP3 Messages

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as clients in your network retrieve them. Even if your company does not use POP3 email, your employees might access their personal POP3 email accounts using mail clients on their computers. Hotmail® or Yahoo® accounts are some examples of POP3 email accounts. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The IMSS POP3 scanner acts as a proxy server (positioned between mail clients and POP3 servers) to scan messages as the clients retrieve them.

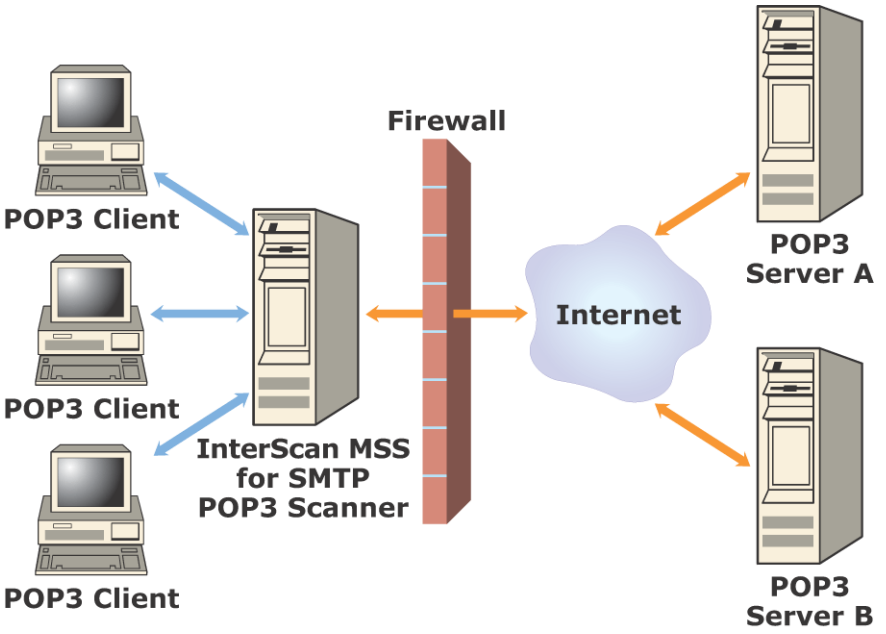


FIGURE 2-1 Scanning POP3 messages

To scan POP3 traffic, configure your email clients to connect to the IMSS server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

You can set up the following connection types:

- **Generic**—Allows you to access different POP3 servers using the same port, typically 110, the default port for POP3 traffic.
- **Dedicated**—Accesses the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure logon, such as APOP or NTLM.

Requirements

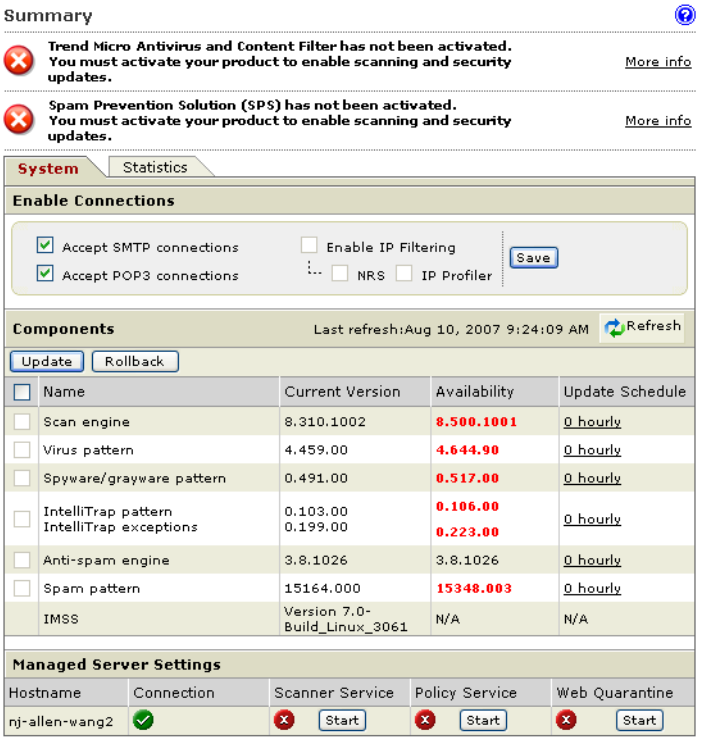
For IMSS to scan POP3 traffic, a firewall must be installed on the network and configured to block POP3 requests from all the computers except IMSS on your network. This configuration ensures that all POP3 traffic passes through the firewall only to IMSS and that IMSS scans the POP3 data flow.

Enabling POP3 Scanning

Before IMSS can begin scanning POP3 traffic, you will need to enable POP3 scanning and configure POP3 settings.

To enable POP3 scanning:

1. Choose **Summary** from the menu. The System tab appears by default.



2. Select the check box next to **Accept POP3 connections**.
3. Click **Save**.

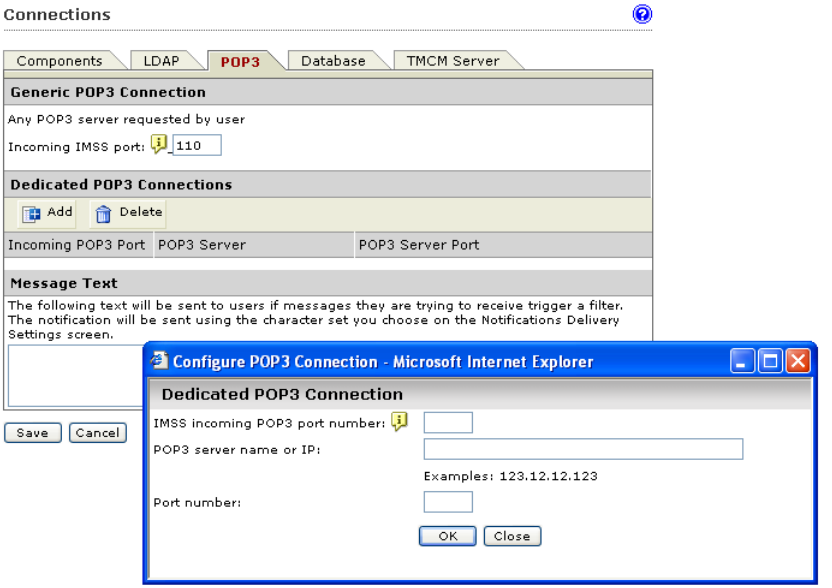
Configuring POP3 Settings

You can specify the IMSS server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection, (through the APOP command or using NTLM) you may also set up a dedicated connection with a customized port assignment.

To add a POP3 connection:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.

2. Click the **POP3** tab.
3. Do one of the following:
   - To accept any POP3 server requested by user, type the incoming IMSS port number, if it is different from the default port 110.
   - To access the POP3 server using a specific port for authentication purposes, click **Add** to create a new dedicated POP3 connection. Provide the required information and click **OK**.



4. Click **Save**.

Managing Policies

IMSS policies are rules that are applied to incoming/outgoing email messages. Create rules to enforce your organization's antivirus and other security goals. This section gives you an overview of how the policy manager enables you to manage IMSS policies.

How the Policy Manager Works

You can create multiple antivirus and other types of rules to filter and reduce security and productivity threats to your messaging system.

An IMSS policy has the following components:

- The **Route**—A set of sender and recipient email addresses or groups to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- The **Filter**—A rule or set of rules that apply to a specific route, also known as scanning conditions. IMSS contains predefined filters that you can use to combat common virus and other threats. You can modify these predefined filters or define your own filters.
- The **Action**—The action that IMSS should take if the filter conditions are met. Depending on the filter result, a filter action is performed that determines how the message is finally processed.

  For more information on how to create a policy, see *Adding Policies* on page 2-34.

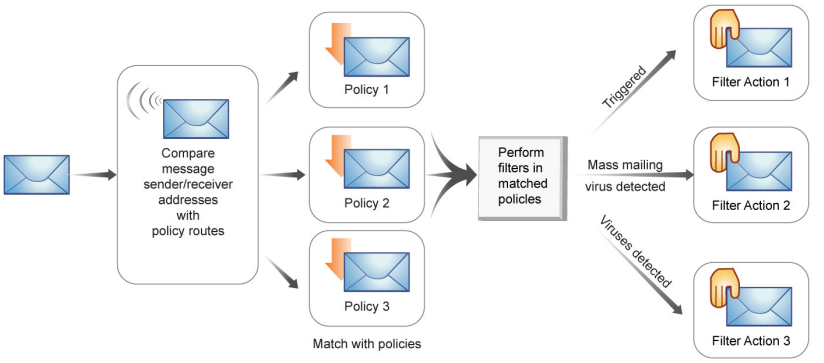


FIGURE 2-2. Simplified policy manager process flow

Understanding Address Groups

An address group is a list of email addresses to which your policy applies.

For example, suppose that you have identified three types of content that you want to block from being transmitted through your company's email system and have defined three filters (in parentheses) to detect these types of content:

- Sensitive company financial data (FINANCIAL)
- Job search messages (JOBSEARCH)
- VBS script viruses (VBSCRIPT)

Now consider the following address groups within your company:

- All Executives
- All HR Department
- All IT Development Staff

The filters that you use in the policies will be applied to these groups as follows:

Address Groups	FINANCIAL	JOBSEARCH	VBSCRIPT
All Executives	Not applied	Applied	Applied
All HR Department	Applied	Not applied	Applied
All IT Development Staff	Applied	Applied	Not applied

Executives, HR staff, and IT developers have legitimate business reasons to send financial information, job search-related correspondence and VBS files, respectively, so you would not apply some filters to those groups.

In IMSS, email addresses identify the different members of your organization and determine the policies that are applied to them. Defining accurate and complete address groups ensures that the appropriate policies are applied to the individuals in those groups.

Managing Address Groups

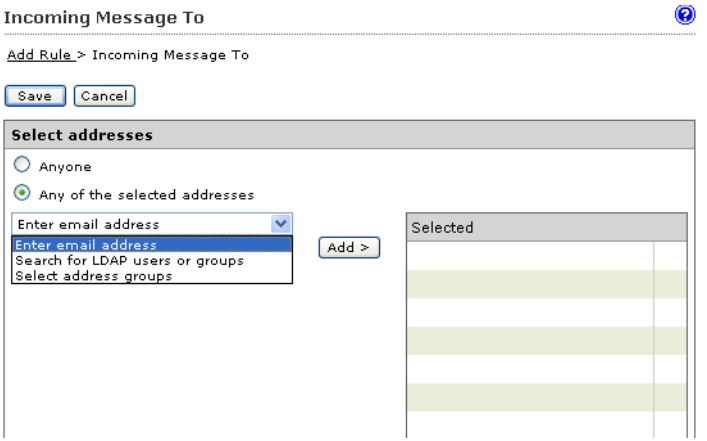
Address groups allow you to organize multiple email addresses into a single group and apply the same policy to every address in the group.

Adding an Address Group

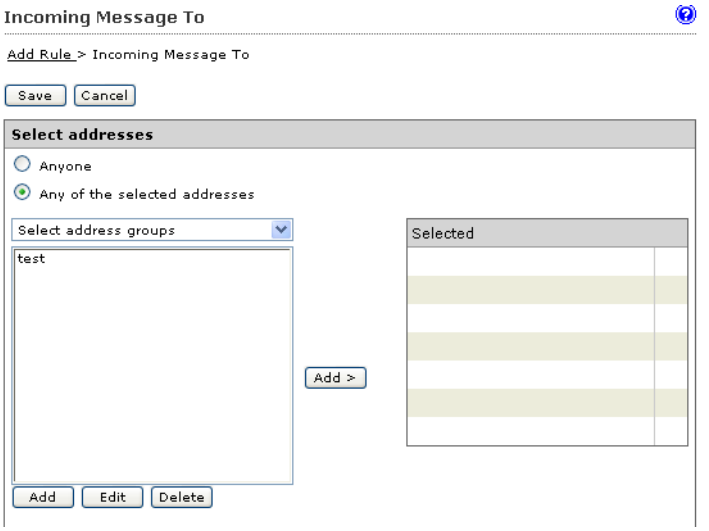
You can create an address group when specifying the route during policy creation. You can also add an address group when modifying an existing policy. This can be done by adding email addresses individually or importing them from a text file. The following provides instructions on adding an address group when creating a new policy.

To add an address group:

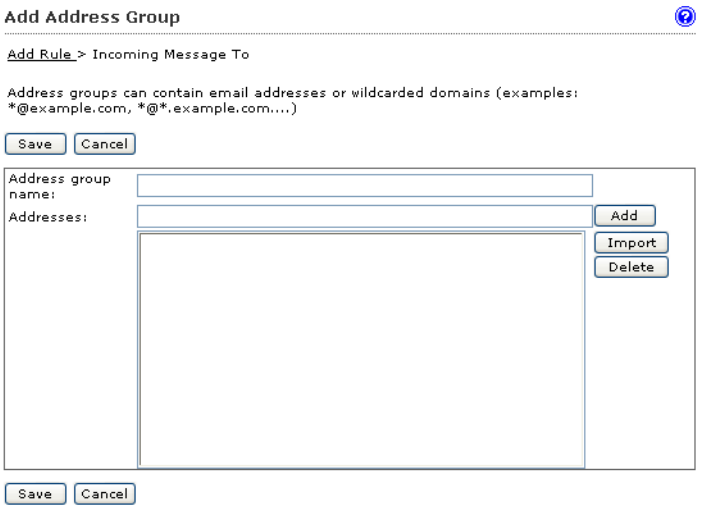
1. Choose **Policy** > **Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the **Recipients** or **Senders** link. The Select Addresses screen appears.



5. Choose **Select Address Groups** from the drop-down list.



6. Click the **Add** button. The Add Address Group screen appears.



7. Type a group name, then do any of the following:

- Type an email address and click **Add** to add email addresses individually. You can also use wildcard characters to specify the email address. For example, *@hr.com.
- Click the **Import** button to import a text file containing a list of predefined email addresses.

Note: IMSS 7.0 can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

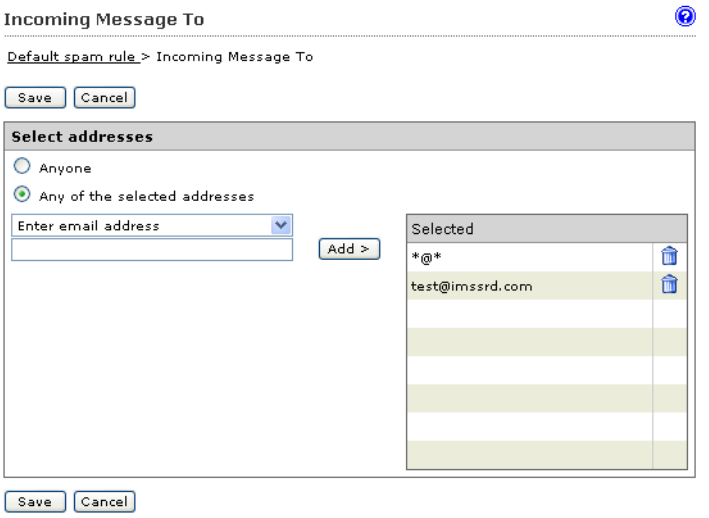
8. Click **Save**.

Editing or Deleting an Address Group

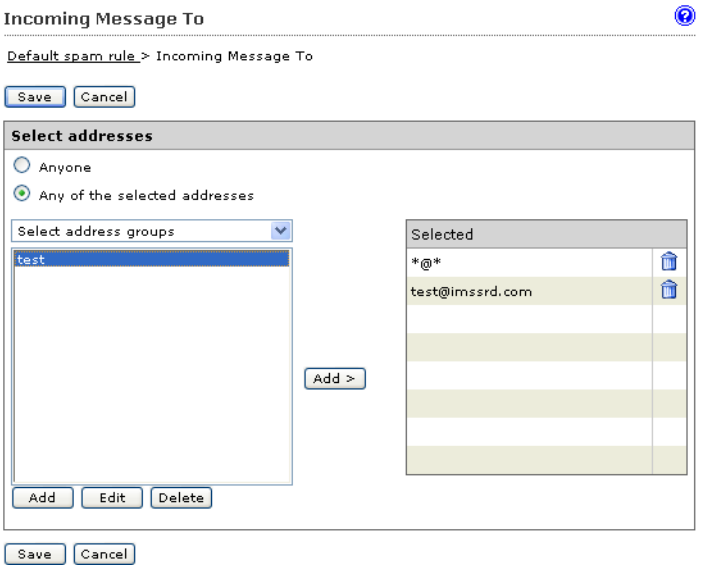
You can edit or delete an address group by editing an existing policy.

To edit or delete an address group:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the link for an existing policy.
3. Click the **If recipients and senders are** link.
4. Click the **Recipients** or **Senders** link. The Select addresses screen appears.



5. Choose **Select address groups** from the drop-down list.



6. Select the desired address group and click the **Edit** or **Delete** button accordingly.

Searching for an LDAP user or group

When specifying the route for a policy, instead of entering an individual email address or address group, you can also perform a search for a Lightweight Directory Access Protocol (LDAP) user or group.

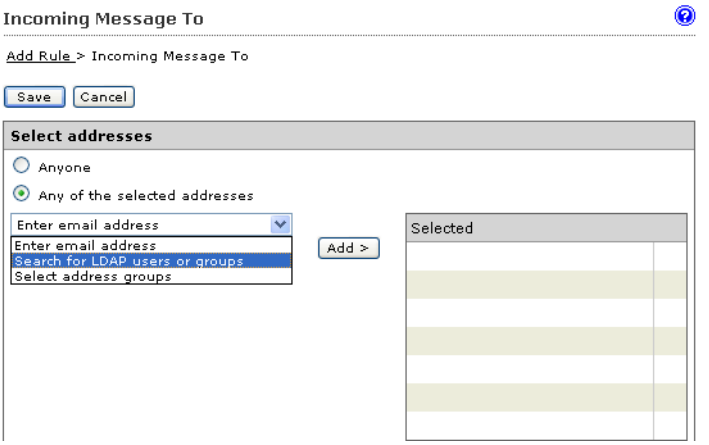
IMSS supports the following three (3) types of LDAP servers:

- Microsoft™ Active Directory 2000 or 2003
- IBM Lotus™ Domino™ 6.0 or above
- SUN™ One LDAP

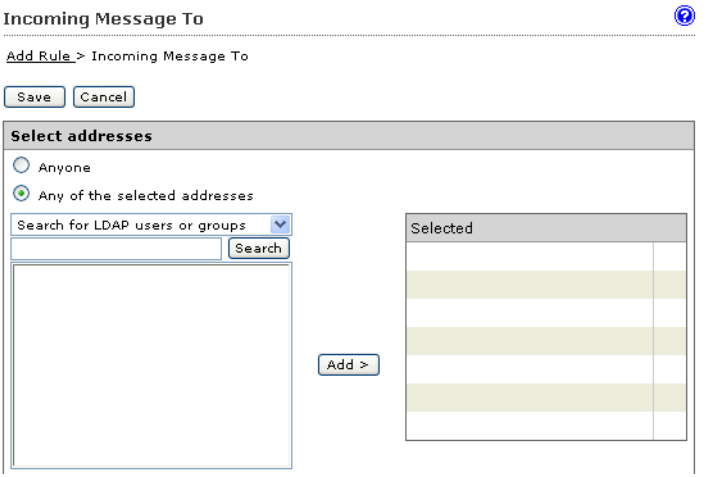
The following steps provide instructions on adding an LDAP user or group when creating a new policy.

To add an LDAP user or group:

1. Choose **Policy** > **Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the **Recipients** or **Senders** link. The Select Addresses screen appears.



5. Choose **Search for LDAP users or groups** from the drop-down list.



6. Type the LDAP user or group that you are looking for.

Note: 1. You can use the asterisk wildcard when performing a search. See *Using the Asterisk Wildcard* on page 2-53.

2. You can also search for LDAP groups when adding internal addresses. For more information, see *Configuring Internal Addresses* on page 2-32.

7. Click the **Search** button.
8. IMSS will display the LDAP user or group if a matching record exists on the LDAP server.
9. Select the user or group and click the **Add** button to add it to the recipient or sender list.

Configuring Internal Addresses

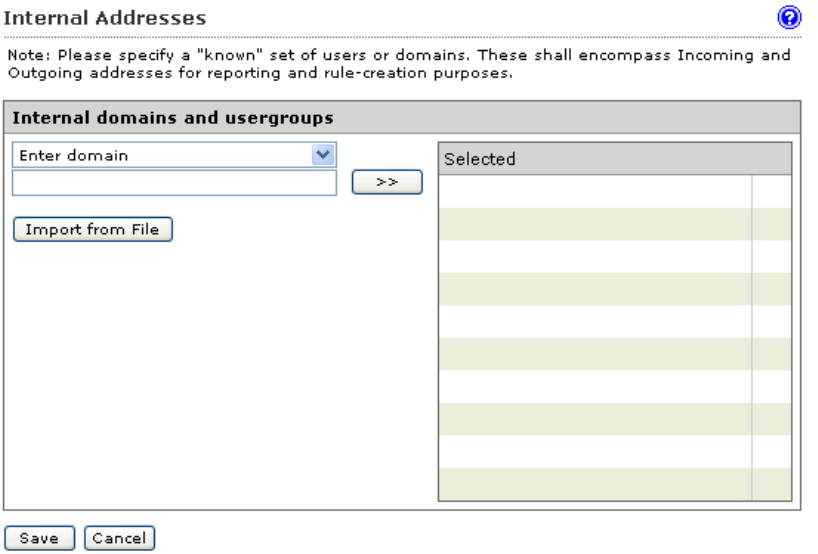
For reporting and rule creation, IMSS uses internal addresses to determine which policies and events are Inbound and Outbound.

Senders and recipients must be on the Internal Addresses list if you select incoming messages or outgoing messages when adding a new rule or modifying an existing rule:

- If you are configuring a rule for outgoing messages, the Internal Address list applies to the senders.
- If you are configuring a rule for incoming messages, the Internal Address list applies to the recipients.

To set internal addresses:

1. Choose **Policy > Internal Addresses** from the menu. The Internal Addresses screen appears.



2. Do any of the following:

- Type an internal domain name and click the >> button to add the domain to the list of internal addresses.

Note: You can also search for LDAP groups when adding internal addresses. For more information, see *Searching for an LDAP user or group* on page 2-30.

- Click the **Import from File** button to import a list of internal domains from a text file.

3. Click **Save**.

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For more information, see *Configuring Internal Addresses* on page 2-32.

Creating a policy involves four (4) steps:

Step 1: Specifying a Route

Step 2: Specifying Scanning Conditions

Step 3: Specifying Actions

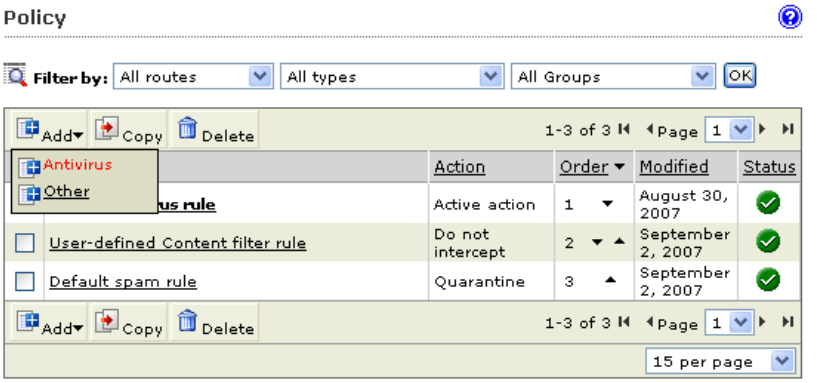
Step 4: Specifying Priority

Tip: To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to "all messages". Select "all messages" from the drop-down list when specifying the route for an antivirus rule.

Specifying a Route

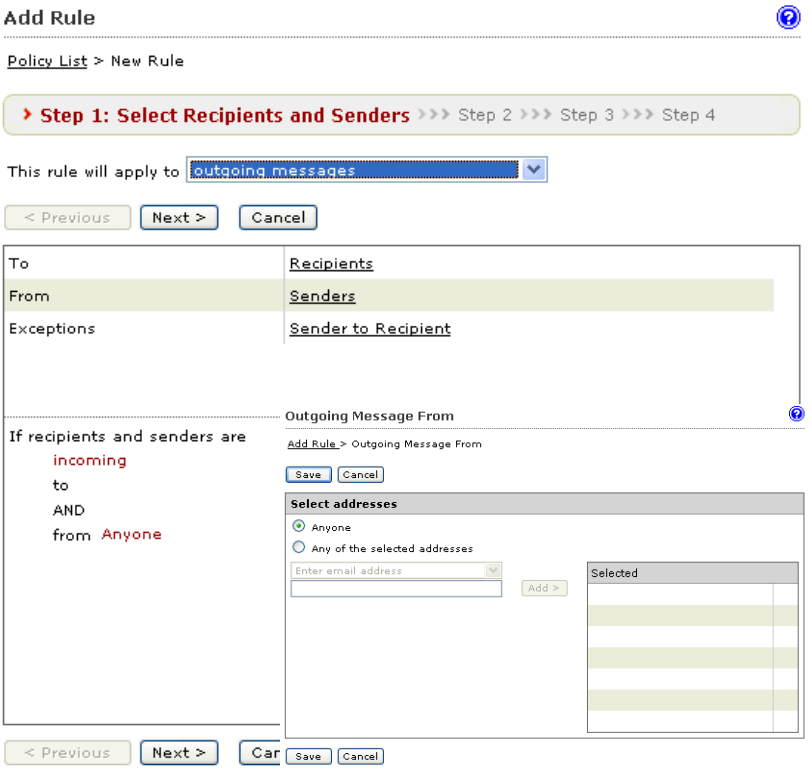
To add a new policy:

1. Choose **Policy > Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.
3. Select **Antivirus** or **Other** from the drop-down list.



Note: The Antivirus rule scans messages for viruses and other malware such as spyware and worms.
The Other rule scans spam or phishing messages, message content, and other attachment criteria.

4. The Add Rule screen appears.



5. Select the policy route type from the drop-down list next to **This rule will apply to**.
   - incoming messages
   - outgoing messages

- both incoming and outgoing messages
- POP3
- all messages (only available when creating an antivirus rule)

6. Select the recipients and senders:
   - For incoming messages, specify the recipient's address, which is in range of the internal addresses. (for example: internal address is *@imsstest.com, valid recipients include jim@imsstest.com, bob@imsstest.com)
   - For outgoing messages, specify the sender's address, which is in range of the internal addresses. (for example: internal address is *@imsstest.com, valid senders include jim@imsstest.com, bob@imsstest.com)
   - For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

Note: 1. You can use the asterisk wildcard when specifying an email address. For more information, see *Using the Asterisk Wildcard* on page 2-53.

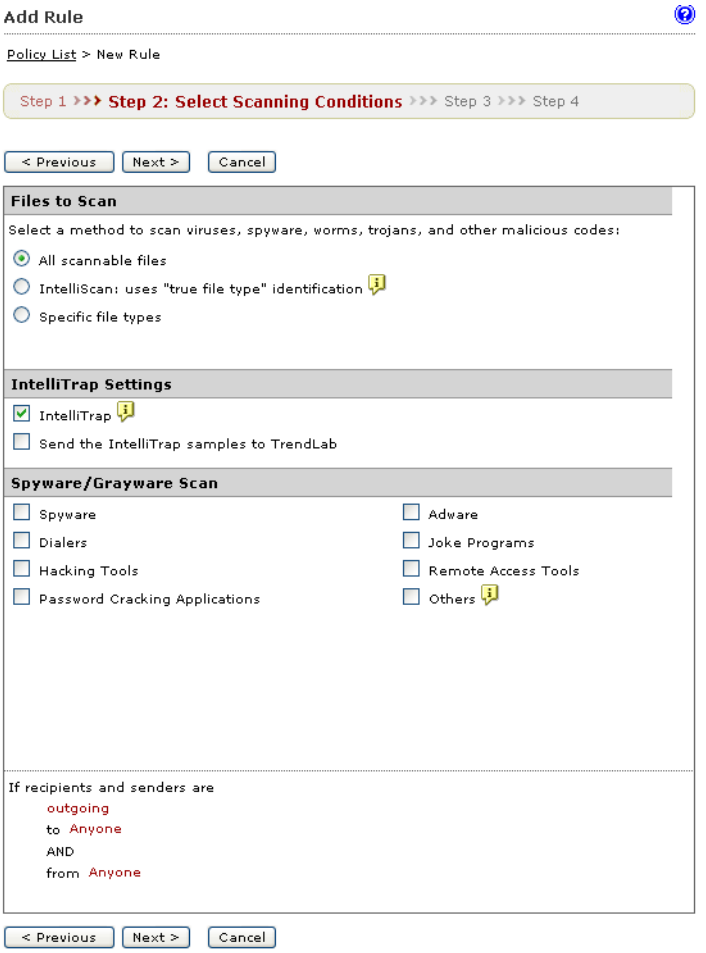
2. If you you selected POP3, you cannot configure the route. The rule applies to all routes.

3. If you selected "all messages" for an antivirus rule, the rule also applies to messages from any sender to any recipient.

Specifying Scanning Conditions

To specify scanning conditions:

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Select the check boxes as desired. The categories of scanning conditions for the Antivirus and the Other rule types vary as follows:



- **Antivirus rule**
  - **Files to Scan**—Sets the default method for scanning messages and specific file types containing viruses and other malware. Also uses IntelliScan to identify malicious code that can be disguised by a harmless extension name.

- **Intellitrap Setting**—Scans compressed files for viruses/malware and sends samples to TrendLab for investigation.
- **Spyware/Grayware Scan**—Scans other types of threats such as spyware and adware.

- **Other rule**
  - **Spam/phishing emails**—Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited messages

containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.

- **Attachment**—Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.
- **Size**—Scans messages that match the specified message size.
- **Content**—Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header or attachment content keyword expressions links.
- **Others**—Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.

Specifying Actions

To set the actions:

1. Click **Next**. The Step 3: Select Actions screen appears.

Note: The user interface that appears in this step depends on the type of rule that you are creating. The antivirus rule contains two tabs that allow you to configure the main actions and the actions for special viruses.

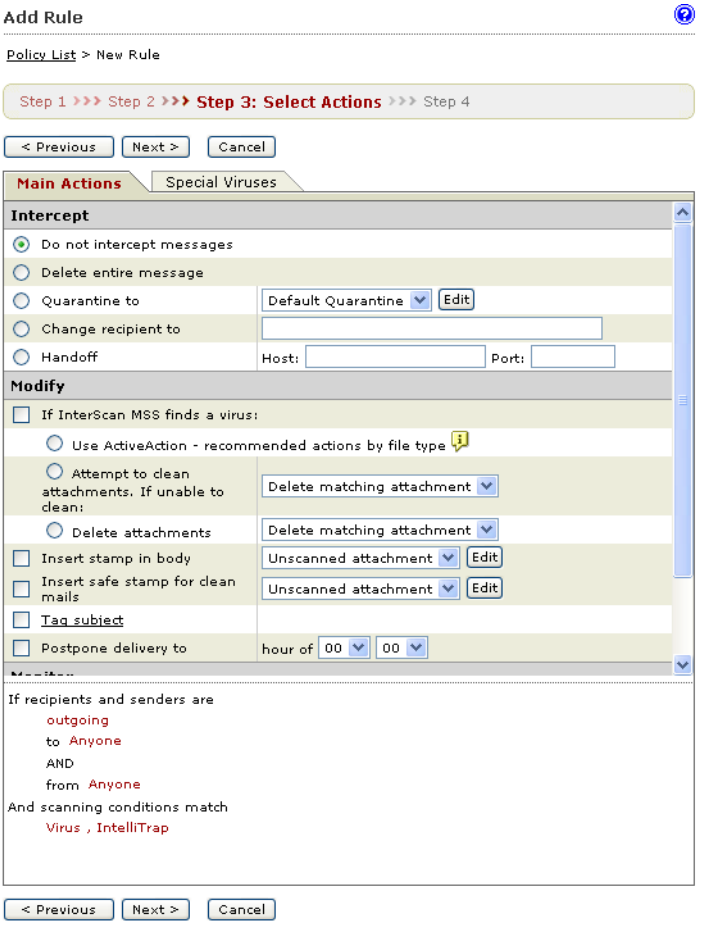
---

2. The main actions for both the Antivirus and Other rule are similar, although there are minor differences in the options listed. Select the desired action(s) from the following categories:
   - **Intercept**—Allows you to choose whether you would like IMSS to intercept the messages and prevent them from reaching the recipients. Choosing the intercept option allows you to specify an action for IMSS to take on intercepted messages.
   - **Modify**—Instructs IMSS to make some alterations to the messages or the attachments, such as inserting a stamp or tagging the subject.
   - **Monitor**—Instructs IMSS to send a notification, archive or blind copy the messages if you would like to further analyze them.

To specify actions for an Antivirus rule:

Specify the main actions or actions for special viruses by clicking the respective tabs.

1. **Main Actions**—Allows you to specify the default actions that IMSS takes when messages match the scanning conditions specified in Step 2: Scanning Conditions.



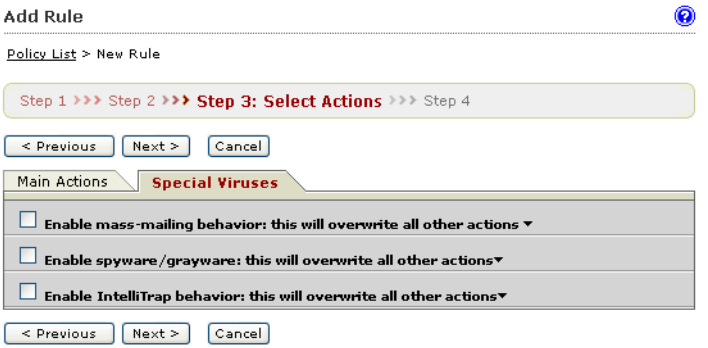
2. **Special Viruses**—Allows you to specify the actions that IMSS takes if the messages match any of the following criteria. The actions specified on this screen will override the default actions specified on the Main Actions tab.

- **Mass mailing**—IMSS takes the actions specified in this section if it detects mass mailing messages.
- **Spyware/grayware**—Allows you to specify the corresponding actions if you have selected any of the Additional Threats Scanning options on the Scanning Conditions screen in step 2. See *Specifying Scanning Conditions* on page 2-36. If IMSS detects spyware/grayware in a message, it takes the actions that are specified here.

Note: IMSS takes the default action for messages matching the Additional Threats Scanning conditions if you do not select alternative actions.

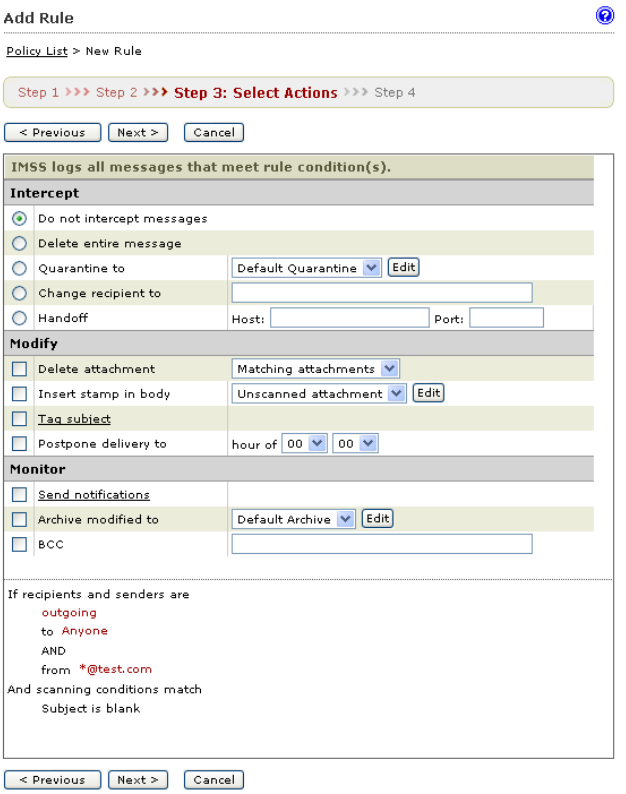
- **IntelliTrap**—Allows you to specify the corresponding actions if you have selected the IntelliTrap Setting options on the Scanning Conditions screen in step 2. See *Specifying Scanning Conditions* on page 2-36.

Note: IMSS takes the default action for messages matching the IntelliTrap conditions if you do not select alternative actions.



To specify actions for the Other rule:

The Select Actions screen when creating an Other rule appears as follows.

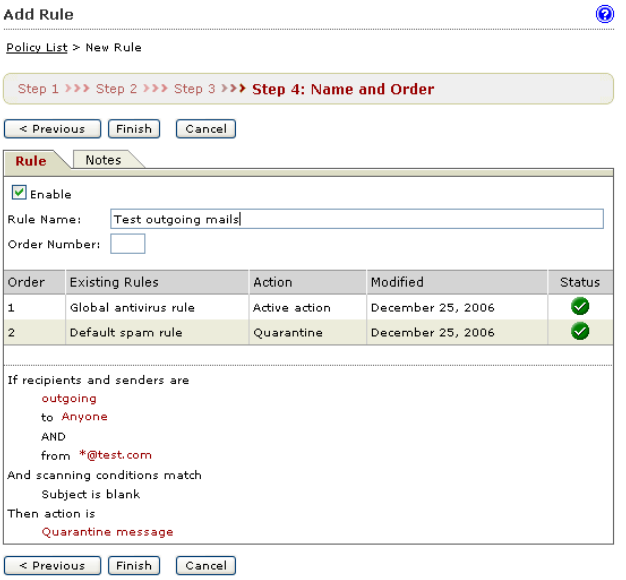


Specifying Priority

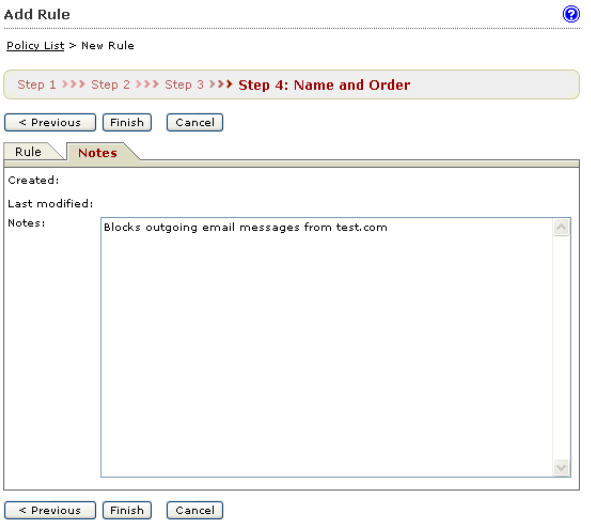
Setting the priority of a rule allows you to control the order in which IMSS matches the messages against a list of policies that you have created.

To specify a priority:

1. Click **Next**. The Step 4: Name and Order screen appears.



2. Select the **Enable** check box to activate the rule.
3. Type a name for the rule in the **Rule Name** field.
4. In the **Order Number** field, specify the priority in which IMSS will perform the scan. IMSS applies the rule to messages according to the order you specify.
5. Click the **Notes** tab. The Notes screen appears.



6. Type a note to distinguish the new rule from other rules.
7. Click **Finish**.

Example 1

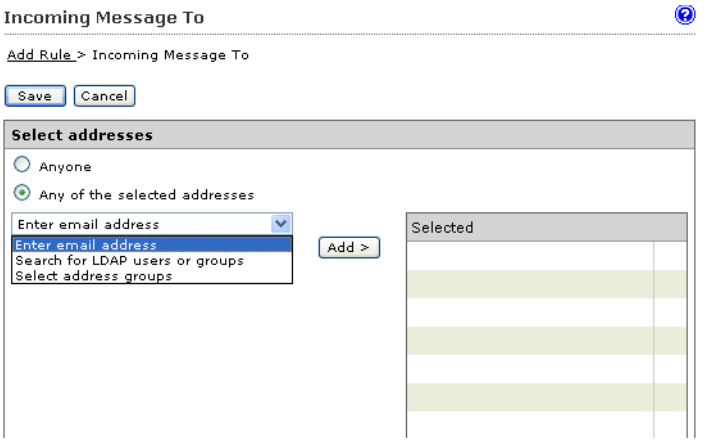
How do I create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients?

Step 1: Specify the Route

1. Choose **Policy** > **Policy List** from the menu.
2. Click **Add**.
3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link. The Select addresses screen appears.
   a. To apply this rule to any recipients, select **Anyone**.

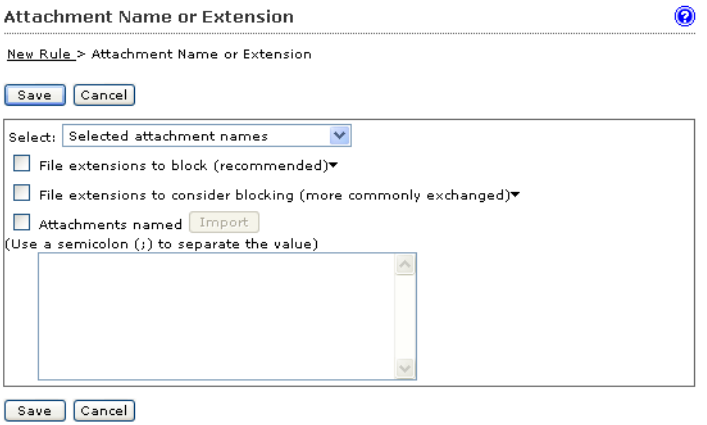
b. To apply this rule to specific recipients, choose **Any of the selected addresses**, and then specify the target email address or group.

c. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.



Step 2: Specify the Scanning Conditions

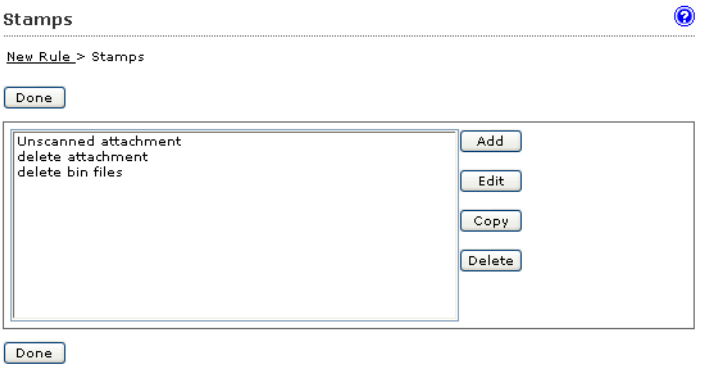
1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Name or extension** condition, select the check box next to it.
4. Click **Name or extension**. The Attachment Name or Extension screen appears.



5. Select the file extensions to block or consider blocking.
6. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.

Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.
3. Select **Matching attachment** from the drop-down list if it is not already selected.
4. Select the check box next to **Insert stamp in body.**
5. If there is no suitable stamp available from the drop-down list, click **Edit**. The Stamps screen appears.



6. Click **Add** to create a new stamp. The New Stamp screen appears.

7. Provide the required information.
8. Click **Save**. The Stamps screen re-appears.
9. Click **Done**. The Select Actions screen re-appears.
10. Select the newly created stamp from the drop-down list.

Step 4: Specify the Priority

1. Click **Next**. The Step 4: Name and Order screen appears.

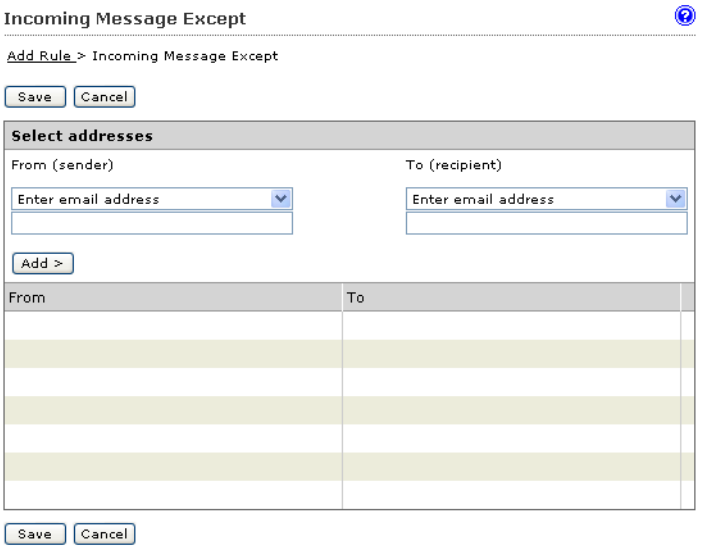
2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

Example 2

How do I create a rule that quarantines messages containing specific keywords in the subject or body and then apply this rule to all recipients except administrators?

Step 1: Specify the Route

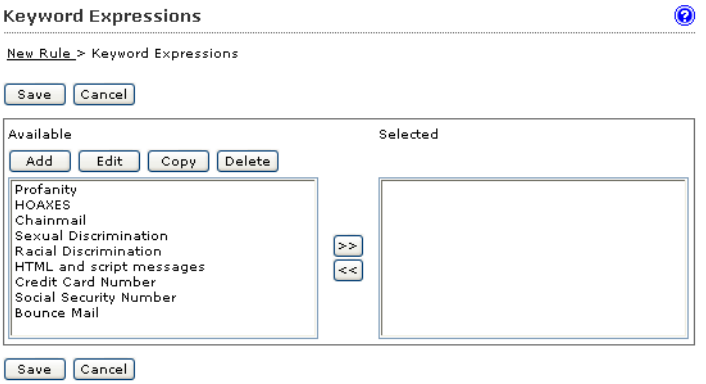
1. Choose **Policy** > **Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.
3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link. The Select addresses screen appears.
6. Select **Anyone**.
7. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.
8. Click the **Sender to Recipient link** next to **Exceptions**. The Exceptions screen appears.



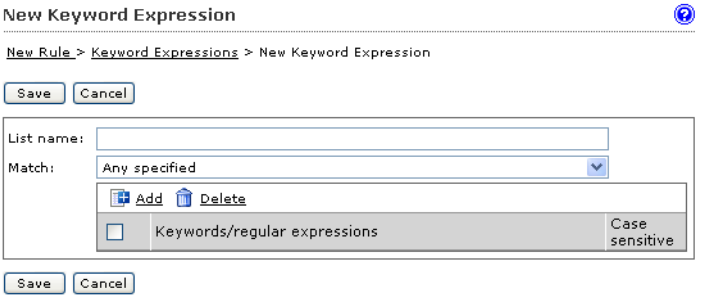
9. Under **From (sender)**, type ***@*** to specify any sender.
10. Under **To (recipient)**, type the administrator's email address.
11. Click **Add**. The sender-recipient pair appears in the list.
12. To add other administrators or recipients, repeat steps 9 to 11.
13. Click **Save** after you finish adding all the desired recipients. The Step 1: Select Recipients and Senders screen re-appears.

Step 2: Specify the Scanning Conditions

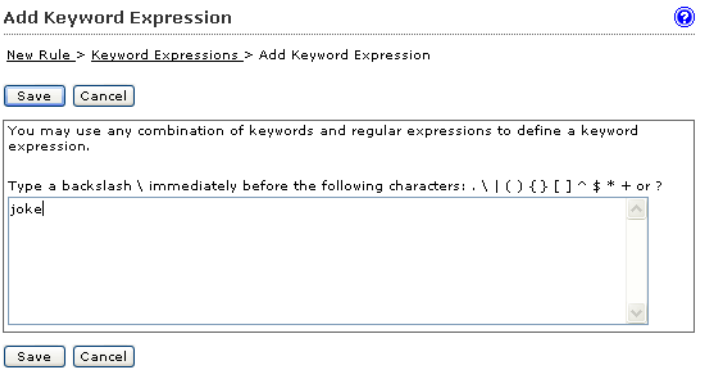
1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**. The Keyword Expressions screen appears.



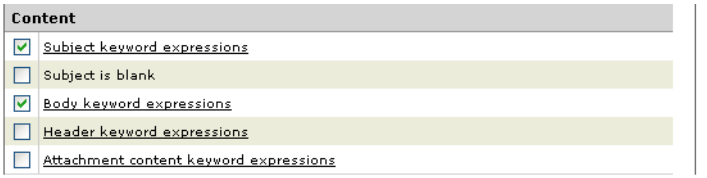
5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list. The New Keyword Expression screen appears.



6. Specify the required information.
7. To add an individual keyword expression, click **Add**. The Add Keyword Expressions screen appears.



8. Type the desired keyword expression and click **Save**. The New Keyword Expression screen re-appears.
9. Repeat steps 7 and 8 for additional keyword expressions.
10. After you have added all the required keyword expressions, click **Save**. The Keyword Expressions screen re-appears with the newly created keyword list.
11. Select the new list and click >> to insert the list into the Selected box.
12. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.
13. To enable the **Body Keyword Expression** condition**,** select the check box next to it.
14. Click **Body Keyword Expression**. The Keyword Expressions screen appears.
15. Select the new keyword list and click >> to insert the list into the Selected box.
16. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears. Ensure that both the Subject keyword and Body keyword expressions are selected.



Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Intercept**, select **Quarantine to**.
3. Accept the **Default Quarantine** area or click the drop-down list to select the desired quarantine area.

Step 4: Specify the Priority

1. Click **Next**. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes and in file names.

Wildcards in Email Addresses

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- ***—Valid representation of all email addresses.
- ***@domain.tld, name@*.tld**—Valid representation of the whole name or the domain (not the top level domain (TLD)).
- ***@*.tld**—Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- **name@domain.*.tld**—Invalid representation of a subdomain.
- **name@domain.***—Invalid representation of a TLD.
- ***name@domain.tld**—Invalid use in conjunction with a name.

Wildcards in File Names

You can use wildcard characters in file names the same way you can use them in email addresses. Use an asterisk in the name or the extension sections of a filename,

but not in conjunction with a partial name or extension. The following are valid examples:

- ***.***—Valid representation of all files.
- ***.extension***—Valid representation of all files of a certain extension.
- **name.***—Valid representation of files with a specific name but with any extension.

The following are invalid examples:

- ***name.***—Invalid representation of a name.
- **name.*extension**—Invalid representation of an extension.

Updating Scan Engine and Pattern Files

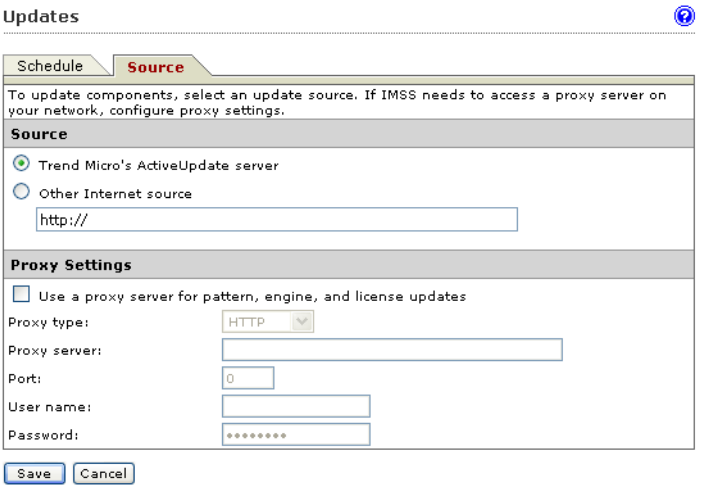
To ensure that your network is constantly well-protected against the latest malware, ensure that you update IMSS components such as the scan engine and virus pattern files on a regular basis. You can choose to perform a manual or scheduled update of the components.

Specifying an Update Source

Before you can update the IMSS scan engine and pattern files, you need to specify the update source. By default, IMSS downloads components from the Trend Micro ActiveUpdate server, which is the only source for up-to-date components. However, if you are using Trend Micro Control Manager (TMCM) to manage IMSS, you can update the components from the Control Manager server.

If you did not specify the Update Source when configuring IMSS using the Configuration Wizard, enter the update source and/or any proxy settings as follows:

1. Choose **Administration** > **Updates** from the menu. The Updates screen appears.
2. Click the **Source** tab.



3. Make your selection and provide the required information.

4. Click **Save**.

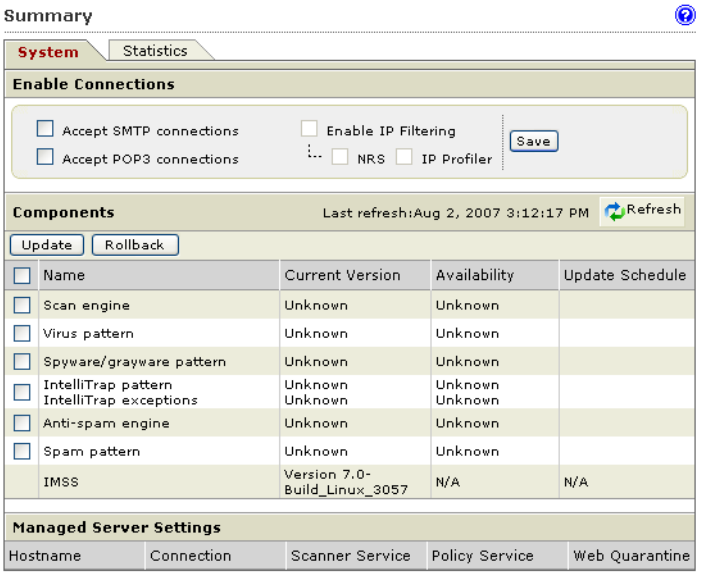
Performing a Manual Update

You may perform a manual update of IMSS components under the following circumstances:

- If you have just installed or upgraded IMSS.
- If you suspect that your network's security is compromised by new malware and would like to update the components immediately.

To perform a manual update:

1. Choose **Summary** from the menu. The Summary screen appears with the **System** tab selected by default.



2. To update all components, select the first check box on the column header next to the Name field. Otherwise, to update specific component(s), select the check box next to the desired component.

3. Click the **Update** button.

Rolling Back a Component Update

If you encounter any system issues after updating IMSS components, you can roll back to the previous version.

To roll back a component update:

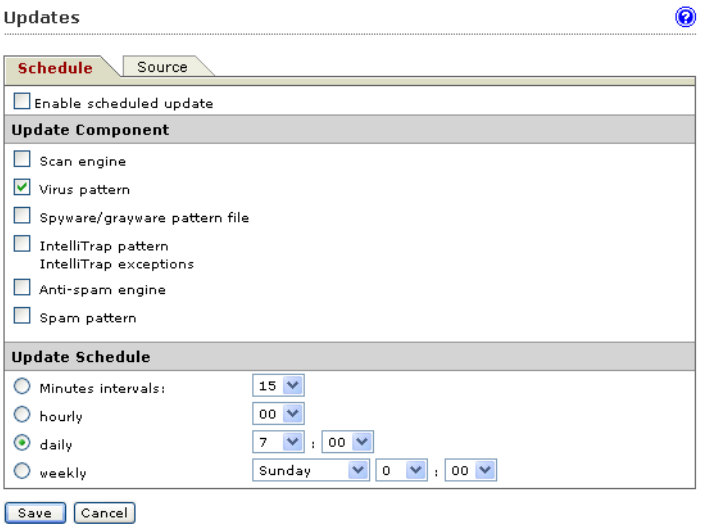
1. Choose **Summary** from the menu. The Summary screen appears with the **System** tab selected by default.
2. To roll back all components to the previous versions, select the first check box on the column header next to the Name field. Otherwise, to roll back specific component(s), select the check box next to the desired component.
3. Click the **Rollback** button.

Configuring Scheduled Update

To have IMSS automatically update the components at specified intervals, configure the update schedule.

To configure a scheduled update:

1. Choose **Administration** > **Updates** from the menu. The Updates screen appears with the Schedule tab selected by default.

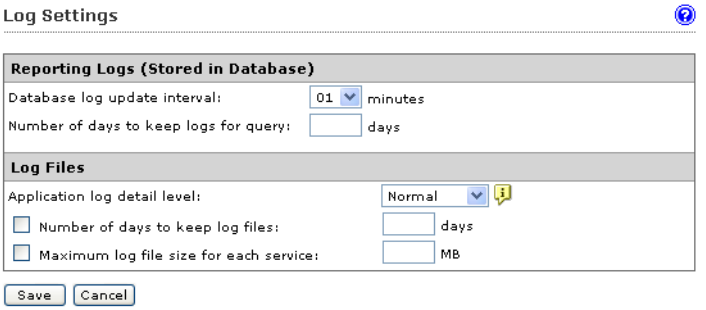


2. Specify the required information.
3. Click **Save**.

Configuring Log Settings

To define the duration for which IMSS retains database logs for query and application logs for troubleshooting purposes, configure the log settings.

1. Choose **Logs** > **Settings** from the menu. The Log Settings screen appears.



2. Specify the required information.
3. Click **Save**.

Chapter 3

Backing Up, Restoring, and Replicating Settings

This chapter provides instructions on how you can back up and restore IMSS configuration settings as a precaution against system failure. If you have deployed multiple IMSS scanners and are using Trend Micro Control Manager simultaneously, you can also replicate IMSS settings without having to reconfigure settings for each new scanner.

Topics include:

- *Backing Up IMSS* on page 3-2
- *Restoring IMSS* on page 3-4
- *Replicating Settings* on page 3-5

Backing Up IMSS

After you have installed IMSS and configured the required settings, it is always prudent to create backups of the settings so that you can restore IMSS quickly in the event of a system failure.

You can choose to perform a full or minimal backup of IMSS as follows:

- **Full**—Backs up all IMSS local configuration and binary files stored in `/opt/trend` and database-related files in `/var/imss`.
- **Minimal**—Backs up only IMSS configuration settings stored in `/opt/trend/imss/config`.

Note: 1. The backup and restore instructions in this manual are targeted at the all-in-one deployment of IMSS. In the case of distributed deployment, you need to backup the following:
a. The database files or tables on the computer(s) where you installed the databases.
b. The local binary and configuration files on every computer where you installed IMSS components.

2. If you perform a minimal backup, you may need to install previous hotfixes, patches, or service packs after restoring IMSS.

To perform a full backup:

1. Stop all IMSS-related processes:
   - `/opt/trend/imss/script/S99ADMINUI stop`
   - `/opt/trend/imss/script/S99IMSS stop`
   - `/opt/trend/imss/script/S99POLICY stop`
   - `/opt/trend/imss/script/S99MANAGER stop`
   - `/opt/trend/imss/script/S99CMAGENT stop`
   - `/opt/trend/imss/script/S99EUQ stop`
   - `/opt/trend/imss/script/S99SCHEDULED stop`
   - `/opt/trend/imss/script/S99FOXDNS stop`
2. Stop Postfix.
3. Back up the folder `/opt/trend/ and /var/imss/`.
4. Back up Postfix configuration file `main.cf` and `master.cf`.

5. Start Postfix.
6. Start all IMSS-related processes:
   - `/opt/trend/imss/script/S99ADMINUI start`
   - `/opt/trend/imss/script/S99IMSS start`
   - `/opt/trend/imss/script/S99POLICY start`
   - `/opt/trend/imss/script/S99MANAGER start`
   - `/opt/trend/imss/script/S99CMAGENT start`
   - `/opt/trend/imss/script/S99EUQ start`
   - `/opt/trend/imss/script/S99SCHEDULED start`
   - `/opt/trend/imss/script/S99FOXDNS start`

To perform a minimal backup:

1. Stop all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.
2. Stop Postfix.
3. Back up `/opt/trend/imss/config` folder.
4. Back up all database tables.
5. Start Postfix.
6. Start all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.

Restoring IMSS

In the event of a system failure, you can restore IMSS depending on whether you have performed a full or minimal backup previously.

To perform full restoration:

1. Install a new IMSS on one computer, ensuring that the IP address, database user name and password are the same as original.
2. Stop all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.
3. Stop Postfix.
4. Restore the folders `/var/imss/` and `/opt/trend/` using the previous backup.
5. Restore Postfix configuration files.
6. Start Postfix.
7. Start all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.

To perform minimal restoration:

1. Install a new IMSS on one computer, ensuring that the IP address, database user name and password are the same as original.
2. Stop all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.
3. Stop Postfix.
4. Restore the `/opt/trend/imss/config/` folder using the previous backup.
5. Restore Postfix configuration files.
6. Import the previous database table backup into the new database.
7. Start all IMSS-related processes. For details, see *To perform a full backup:* on page 3-2.

Replicating Settings

If you have installed multiple IMSS scanners that do not share the same admin database, you can use the Trend Micro Control Manager to replicate settings across these scanners without having to configure each scanner separately. If the scanners share the same admin database, it is not necessary to replicate settings.

Do the following if you intend to replicate settings using Control Manager:

Step1: Back up IMSS settings. For details, see *Backing Up IMSS* on page 3-2.

Step2: Enable the Control Manager agent.

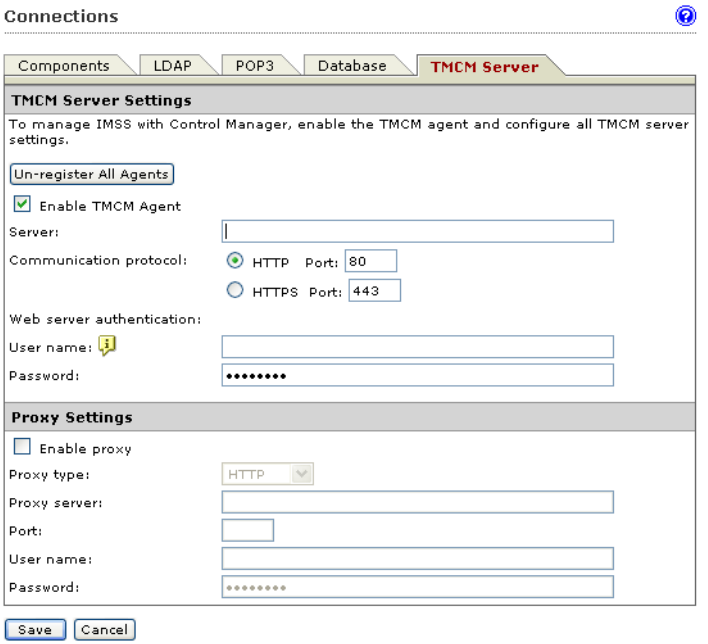
Step3: Replicate settings from the Control Manager Web console.

Enabling Control Manager Agent

IMSS automatically installs the Trend Micro Control Manager agent during installation. To integrate with Control Manager, all you need to do is provide the Control Manager server details and enable the agent from the Web management console.

To configure Control Manager Server settings:

1. Choose **Administration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **TMCM Server** tab. The TMCM Server Settings screen appears.



3. Provide the required information.
4. Select the check box next to **Enable TMCM Agent**.
5. Click **Save**.

Replicating Settings from Control Manager

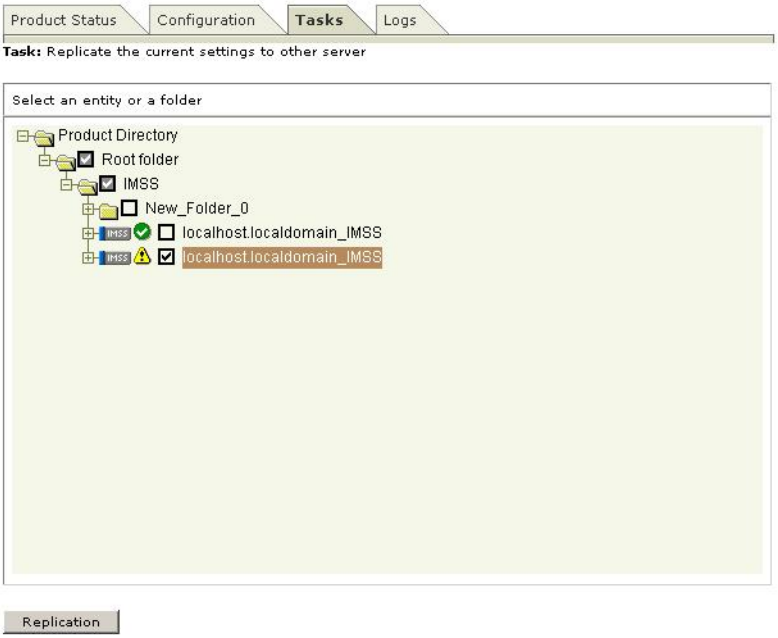
After enabling the Control Manager agent from the IMSS Web management console, you can start to replicate IMSS settings by logging on to the Control Manager Web console.

To replicate IMSS settings:

1. Choose **Products** from the Control Manager menu.
2. Locate the source IMSS scanner from the Product Directory on the left of the user interface.
3. Click the **Tasks** tab.

4. Select **Configuration Replication** from the drop-down list.

5. Click **Next**.
6. Select the check box next to the target server.



7. Click the **Replication** button.

Chapter 4

Maintaining IMSS

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSS. For more information on each field on the Web management console, please refer to the Online Help.

Topics include:

- *Monitoring Your Network* on page 4-2
- *Logs* on page 4-14
- *Quarantine and Archive* on page 4-16
- *Event Notifications* on page 4-24
- *Managing Administrator Accounts* on page 4-29
- *Configuring Scanner and Policy Connections* on page 4-32

Monitoring Your Network

IMSS provides a complete set of tools that enable you to monitor your network traffic. You can obtain useful information such as the statistics on the performance of IMSS components, or generate reports that display a breakdown of messages matching various scanning conditions.

Viewing Statistics

You can obtain up to the last seven days' of statistics on the performances of IMSS scanners and IP profilers. These statistics provide useful information to help you better manage your IMSS policies and enhance the security of your network.

To view the statistics:

1. Choose **Summary** from the menu. The System tab appears by default.
2. Click the **Statistics** tab.
3. Select the desired last # days from the Show drop-down list.

Note: IMSS automatically updates these statistics in its database at a quarter past every hour. You can click Refresh to update the screen, but any newly updated statistics in the database will not display on the screen until IMSS has completed the next hourly database update.

For example, if you click Refresh at 4pm, IMSS will only update the database at the next hourly update at 4:15pm. Assuming IMSS takes 2 minutes to process your request, you will only see the results at 4:17pm.

Interpreting the Statistics

IMSS presents performance statistics in both graphical and table formats. This section explains how the values are derived and helps you to understand the information by breaking down the Statistics tab into the three main sections, which are Performance Overview, Scan Performance, and IP Filtering Performance.

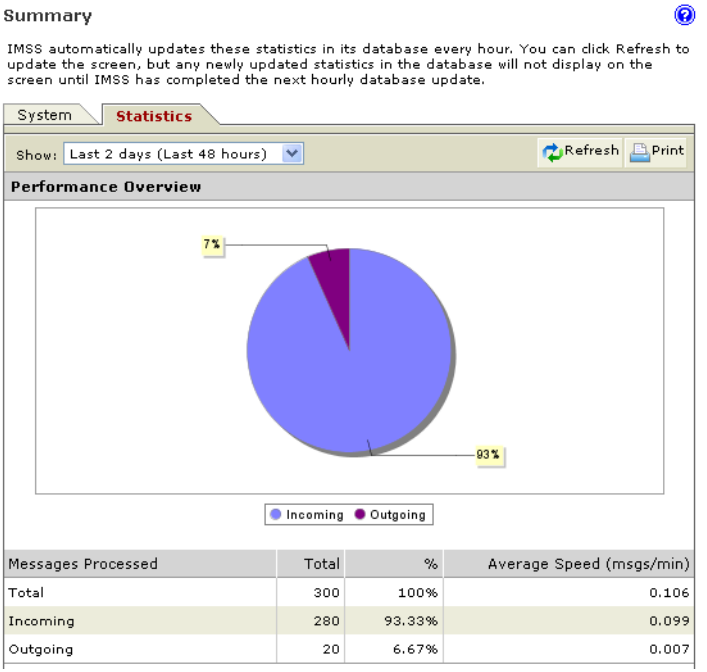
Note: 1. The values (in percentages) for the same type of threat shown in the chart and table are computed differently.

2. In the table, the total number of messages matching each scanning condition or IP filtering type consists of overlaps. For example, if a message matches more than one scanning condition, such as spam and attachment, this message will be counted twice, once in the total number for spam and a second time in the total number for attachment. Values in the chart, however, do not include such overlaps.

Performance Overview

This section shows the total number of incoming and outgoing messages in your network and their corresponding values measured as percentages of the total. The total number includes messages blocked by the following components in ascending order:

- IP Profiler
- NRS
- Scan engine



Scan Performance

This section shows a breakdown of the number of messages matching various types of scanning conditions specified in the policy rules, and their corresponding values in percentages.

- **Chart**

  Value = Number of messages matching the specific scanning condition divided by the number of messages matching all scanning conditions.

  Example:

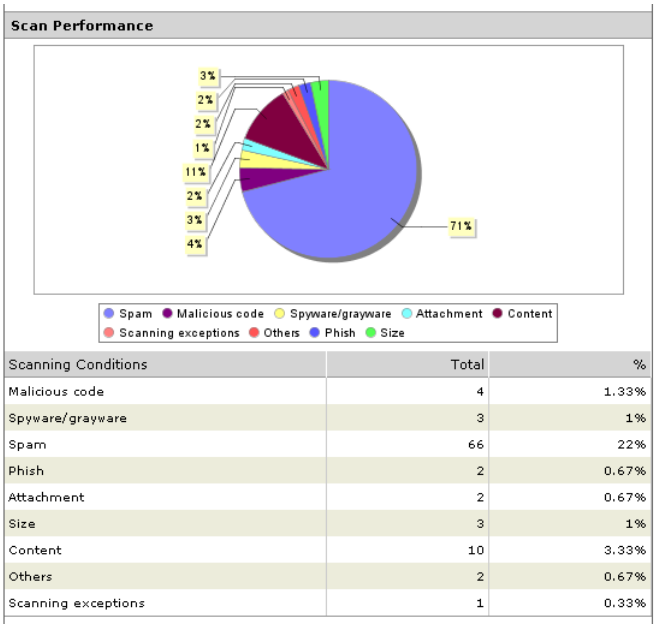
  Percentage of spam messages: 71% = 66 / 93

- **Table**

  Value = Number of messages matching the specific scanning condition divided by the total number of messages processed.

  Example:

  Percentage of spam messages: 22% = 66 / 300



Scanning Conditions	Total	%
Malicious code	4	1.33%
Spyware/grayware	3	1%
Spam	66	22%
Phish	2	0.67%
Attachment	2	0.67%
Size	3	1%
Content	10	3.33%
Others	2	0.67%
Scanning exceptions	1	0.33%

IP Filtering Performance

This section shows the number of connections blocked by the following:

- The four types of IP Filtering rules, namely, spam, virus, DHA attack, and bounced mail
- IP addresses that you have manually entered
- NRS

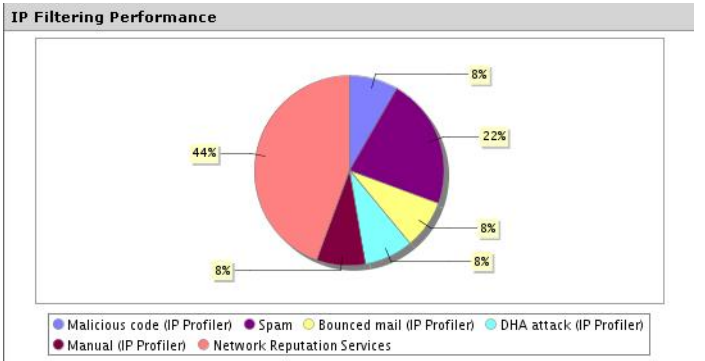
Values in the chart and table are computed as follows:

Value = Number of messages matching the specific IP filtering rule divided by the total number of messages blocked by IP Profiler and NRS.

Example:

Total number of messages blocked by IP Profiler and NRS = 360

Percentage of spam messages: 22% = 80 / 360



IP Filtering Type	Total Blocked Connection	Blocked %
Total	360	100%
Spam (IP Profiler)	80	22.22%
Malicious code (IP Profiler)	30	8.33%
DHA attack (IP Profiler)	30	8.33%
Bounced mail (IP Profiler)	30	8.33%
Manual (IP Profiler)	30	8.33%
Network Reputation Services	160	44.44%

Generating Reports

Depending on your needs, you can choose to generate a one-time report on demand or schedule a report to be run at specific intervals. IMSS offers you the flexibility of specifying the content for each report and the option of viewing or saving the result in HTML or CSV format.

Types of Report Content

You can choose from the following types of content to be included in the report:

Report Content	Descriptions
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages. Also shows the number of messages matching specific scanning conditions.
Virus and malicious code summary	Shows a summary of the virus message count by actions.
Spam summary	Shows a summary of the total spam message count by anti-spam engine, NRS, IP Profiler, and actions.
Sender IP address blocking summary	Includes "IP Profiler Blocking Summary" and "NRS Blocking Summary". The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached NRS and are blocked by NRS.
Top 10 traffic email addresses	Shows the top 10 email addresses ranked by the total sent and received message count.
Top 10 virus names	Shows the top 10 virus names ranked by their detected count.
Top 10 IP addresses for DHA attack addresses	Shows the top 10 IP addresses ranked by the blocked count for DHA attack.
Top 10 IP addresses for bounced mail attack addresses	Shows the top 10 IP addresses ranked by the blocked count for bounced mail attack.
Top 10 virus recipients and senders	Shows the top 10 virus recipients and senders ranked by their total received and sent virus message count respectively.

TABLE 4-1. Report content descriptions

Report Content	Descriptions
Top 10 most frequently triggered rule names	Shows the top 10 rule names ranked by the number of messages that triggered each rule.
Top 10 spam recipients	Shows the top 10 spam recipient addresses ranked by their total received spam message count.
Top 10 IP addresses blocked by NRS	Top 10 blocked IP addresses ranked by the number of connections dropped by NRS.
Top 10 IP addresses blocked by spam	Top 10 IP addresses ranked by the blocked count for spam.
Top 10 IP addresses blocked by viruses or malicious code	Top 10 IP addresses ranked by the blocked count for viruses.

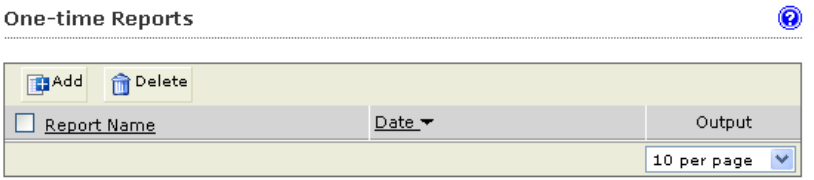
TABLE 4-1. Report content descriptions

Adding One-time Reports

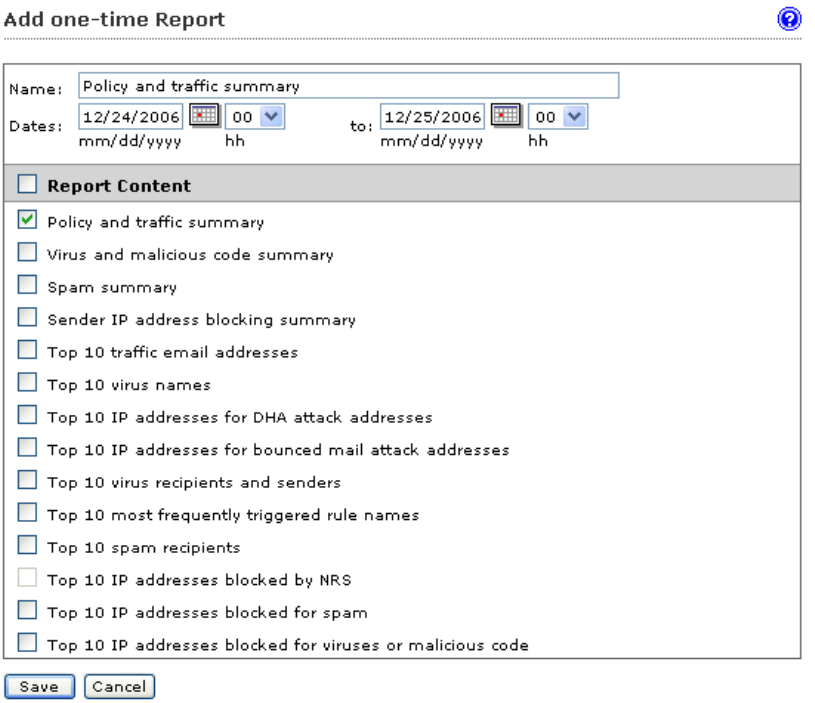
You can generate one-time reports on demand to help monitor the traffic on your network.

To create a one-time report:

1. Choose **Reports > One-time Report** from the menu.

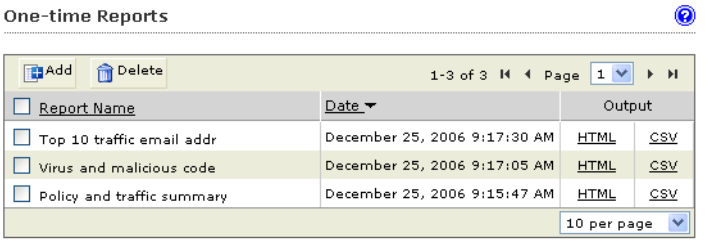


2. Click **Add**.

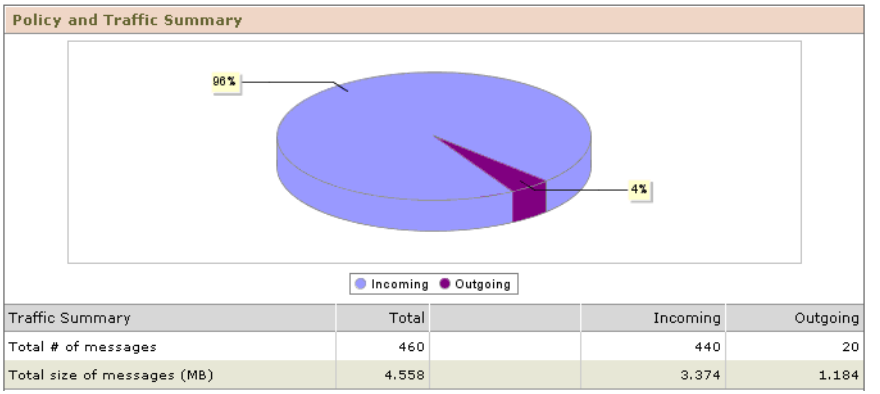


3. Provide the required information.
4. Click **Save**. The report takes several minutes to generate. The message **In progress** appears in the report table.

After the report generates, the hyperlinks **HTML** and **CSV** display in the report table.



5. Click **HTML** to display the report in HTML format.
6. Click **CSV** to export the report data to a csv file.



Traffic Summary	Total		Incoming	Outgoing
Total # of messages	460		440	20
Total size of messages (MB)	4.558		3.374	1.184

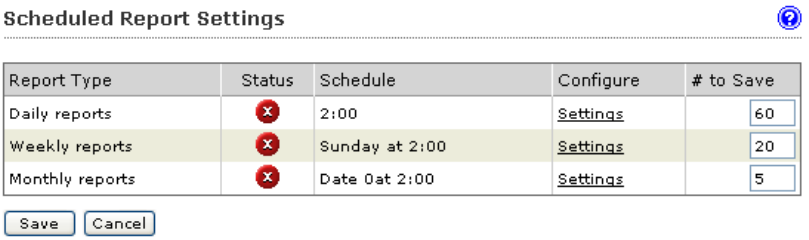
Note: Report generation occurs once every five minutes. This means that report generation could require as much as five minutes in addition to the time required to aggregate reporting data and make the necessary calculations.

Configuring Scheduled Reports

Scheduled reports generate automatically according to the intervals you configure.

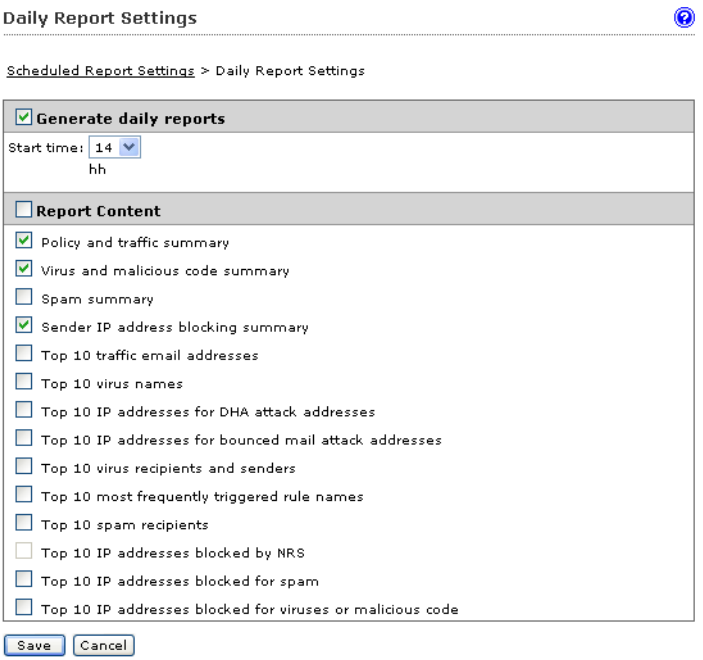
To create a scheduled report:

1. Choose **Reports > Settings** from the menu. The Scheduled Report Settings screen appears.



2. Click the **Settings** link for one of the following report types:
   - Daily reports
   - Weekly reports
   - Monthly reports

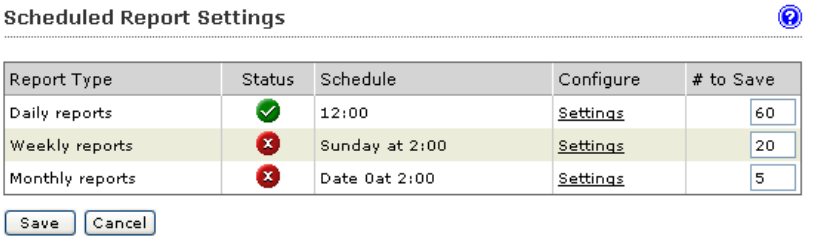
   The Report Settings screen appears.



3. Specify your settings for the report.

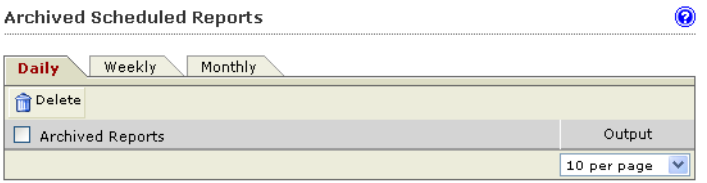
Note: When configuring monthly report settings, if you choose to generate the report on the 29th, 30th, or 31st day, IMSS will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSS will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Click **Save**. The report status changes.

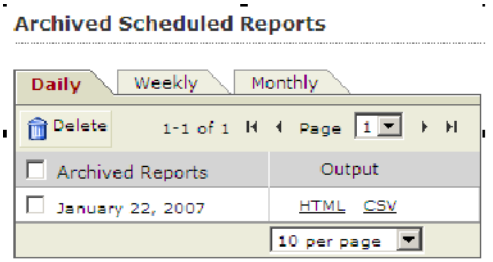


5. Specify the number for each type of report that you would like to retain. Click **Save**.
6. Choose **Reports > Scheduled Reports** from the menu. The Scheduled Reports screen appears.

Note: The report has not generated yet.



7. After the report generates, you can click **HTML** or **CSV** to view the report.


Archived Scheduled Reports
Daily
Weekly
Monthly
Delete
1-1 of 1
Page
1
Archived Reports
Output
January 22, 2007
HTML
CSV
10 per page

Logs

Logs are a useful means of enabling you to monitor various types of events and information flow within IMSS. They also serve as an important resource for troubleshooting purposes.

To enable logs and benefit from the information, do the following:

Step 1: Configure the log settings. For details, see *Configuring Log Settings* on page 2-59.

Step 2: Perform log query.

Querying Logs

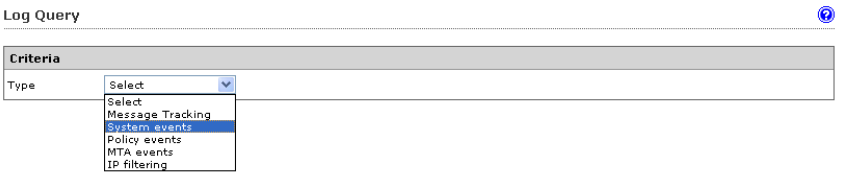
You can perform queries on five types of events or information:

- **Message tracking**—Records message details such as the sender, recipient(s), message size, and the final action that IMSS has taken. In the case of quarantined messages, the query result will also indicate the name and type of the policy rule that was triggered.
- **System events**—Tracks the time of system events such as user access, modification of rules, registration of Control Manager agent and so on.
- **Policy events**—Provides details on the policy rules that were triggered, the actions taken, and the message details.
- **MTA logs**—Provides connection details of Postfix on the local computer where the central controller is installed.
- **IP Filtering**—Provides the time when IMSS started and stopped blocking email messages from the queried IP address.

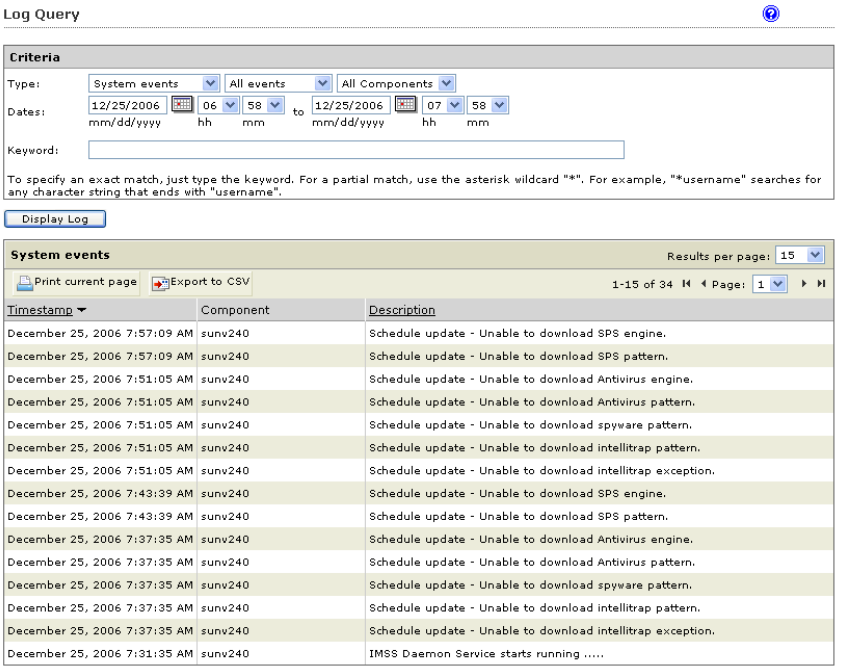
For most log queries, IMSS supports wildcards (*) and exact matches (for example, to view mail recipients whose name includes A or B, set the recipient(s) to "`*A*;*B*`"). IMSS uses exact matching by default. Leaving the search condition blank displays all logs. For multiple-conditions items, use semicolons (;) to separate the entries for recipient(s) and attachment(s).

To query logs:

1. Choose **Logs > Query** from the menu. The Log Query screen displays.
2. Select the type of logs to query from the **Type** drop-down list.



3. Specify the query details.
4. Click **Display Log**.



Quarantine and Archive

Quarantine and archive are among some of the actions that you can configure IMSS to take when messages match certain rules. Generally, you configure IMSS to quarantine messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s). Archive, on the other hand, allows you to store messages for future reference.

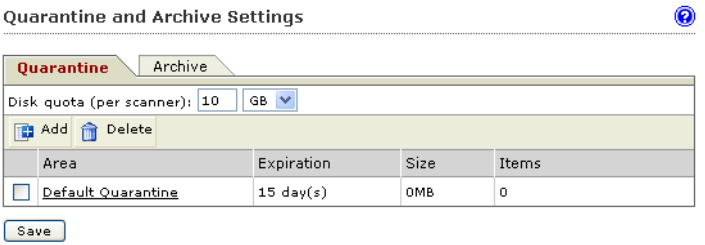
Note: In order to use End-User Quarantine, you must first configure the LDAP settings. For more information, see *Step 3: Configuring the LDAP Settings* on page 1-7.

Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage these areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

To configure quarantine and archive settings:

1. Choose **Quarantine & Archive** > **Settings** from the menu. The Quarantine and Archive Settings screen appears.



2. Specify the disk quota per scanner.
3. Click **Add**. The Add Quarantine screen appears.

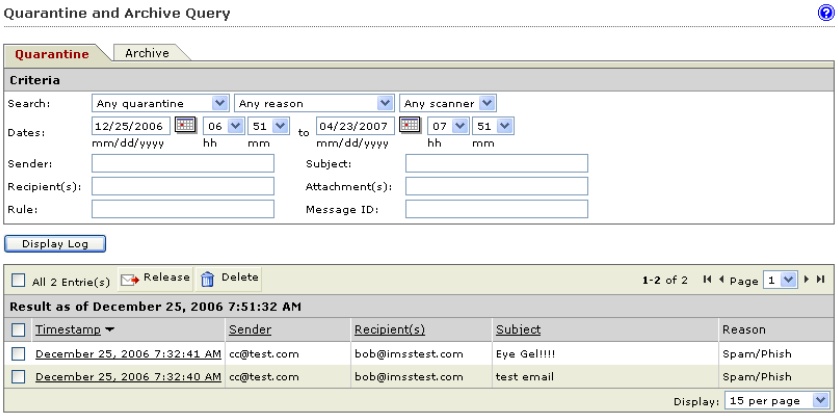
4. Specify the required information.
5. Click **Save**. To configure archive settings, click the **Archive** tab accordingly.

Querying Quarantined and Archived Messages

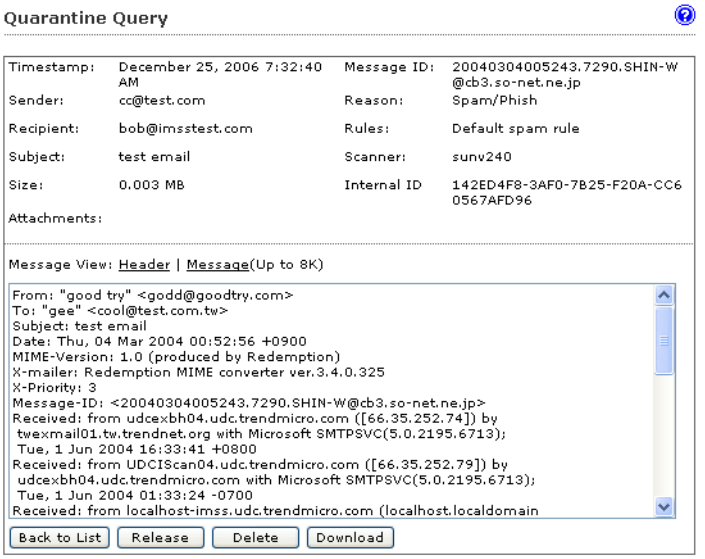
You can perform a query on quarantined and archived messages before deciding on the action to be taken. After viewing the message details, you can choose to release or delete the quarantined messages, or delete archived messages from IMSS.

To manage quarantined or archived email:

1. Choose **Quarantine & Archive > Query** from the menu. The Quarantine and Archive Query screen appears.
2. In the **Quarantine** tab, specify the search criteria.
3. Click **Display Log**.



4. Click on the timestamp hyperlink for a result item. The item details display in the Quarantine Query screen.



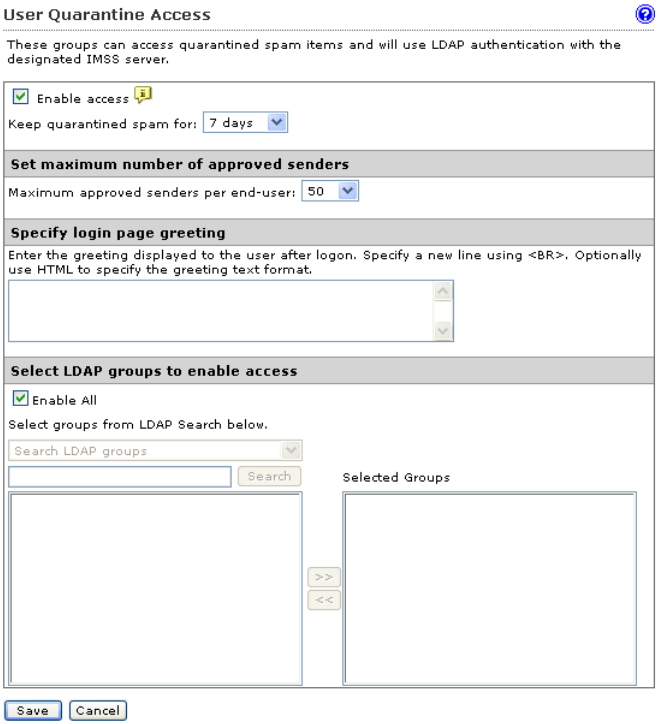
5. Click **Release** or **Delete** to release or delete the email from the quarantine respectively.
6. To query archived messages, click on the **Archive** tab on the Quarantine & Archive screen, then specify the search criteria accordingly.

Configuring User Quarantine Access

You can grant all users or selected end-users access to the EUQ Web console so that they can manage the spam messages addressed to them by visiting `https://<target server IP address>:8447`.

To configure user quarantine access:

1. Choose **Administration** > **User Quarantine Access** from the menu. The User Quarantine Access screen appears.



2. Specify the desired settings.
3. Select the **Enable access** check box to activate the feature.
4. Click **Save**.

Adding/Removing an EUQ Database

If you have an existing EUQ database, you may add new EUQ databases if you want to do the following:

- To perform load balancing
- To allow more end-users to access EUQ.

Alternatively, you may choose to reduce the number of EUQ databases.

Adding an EUQ Database

Perform the following to add an EUQ database.

Step 1: Set up the EUQ database

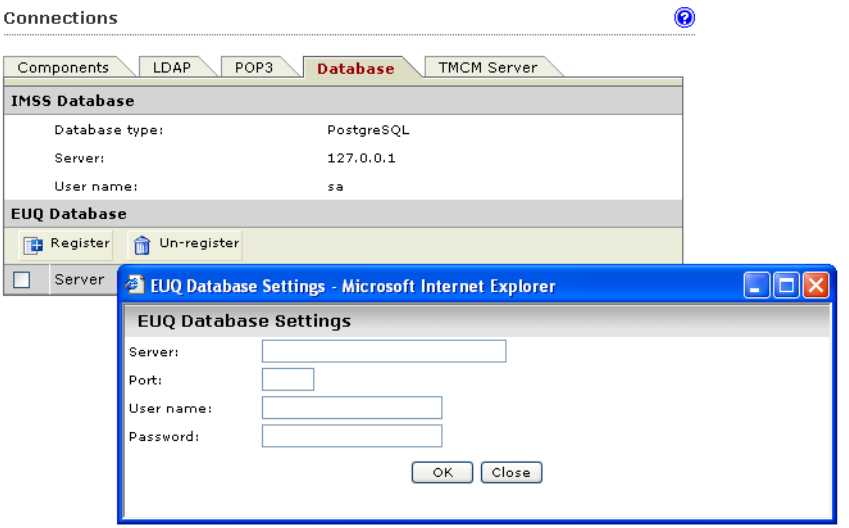
Step 2: Rebuild end-user data

Step 1: Set up the EUQ database

You may register an EUQ database from the Web management console if the database was already installed but unregistered. Otherwise, please run the IMSS installation program to add a new EUQ database to the system.

To register an EUQ database:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **Database** tab.
3. Click the **Register** button. The EUQ Database Settings screen appears.



4. Provide the required information.
5. Click **OK**.

Step 2: Rebuild end-user data

To retain the original end-user's data, run the `euqtrans` script from the `<IMSS>\script` directory of the Central Controller to re-balance the EUQ databases. This script does the following:

- Transfer the Approved List
- Transfer information about the quarantined emails

Note: If you do not run the euqtrans script after adding the new EUQ Database, some previously quarantined mail messages may not be available to the end-users.

Removing an EUQ Database

Perform the following to remove an EUQ database.

Step 1: Remove the EUQ database

Step 2: Rebuild end-user data

Step 1: Remove the EUQ database

You can unregister but not delete the EUQ database from the system via the Web management console. Unregistering a database means that the database will still be there, but it will not be used by IMSS.

To unregister an EUQ database:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.
2. Click the **Database** tab.
3. Select the check box next to the unwanted EUQ database server.
4. Click **Unregister**.
5. Click **OK** to confirm the unregistration.

Step 2: Rebuild end-user data

Run the `euqtrans` script from the `<IMSS>\script` directory of the Central Controller to move the Approved Senders List and information about the quarantined mail messages from this database to other databases and re-balance the other databases.

Command-line options for euqtrans tool

The command-line options for the euqtrans script are as follows:

all—Transfer the individual Approved Senders Lists and information about the quarantined mail messages from the database that was removed to the new location (database) based on the updated Table and Database mapping.

approvedsender—Transfer the individual Approved Senders Lists from the database that was removed to the new location (database) based on the new mapping.

Event Notifications

You can configure IMSS to send an email or SNMP notification to you or specific email users upon the occurrence of the following categories of event:

- **System Status**—Informs you when certain IMSS performances fall below the desired level. For example, when a scanner service stops working, or when the number of messages in the delivery queue exceeds the desired quantity.
- **Scheduled Update Event**—Alerts you when IMSS is able or unable to perform a scheduled update of the scan engine or pattern files from the update source onto the admin database.
- **Scanner Update Result**—Alerts you when IMSS is unable to update the engine or pattern files on any scanner.

Note: Component update is a 2-step process:
1. At the scheduled time, the IMSS admin database will first check the update source for new engine or pattern files.
2. IMSS scanners will then check the admin database at regular intervals for updated components. The default interval is three (3) minutes.

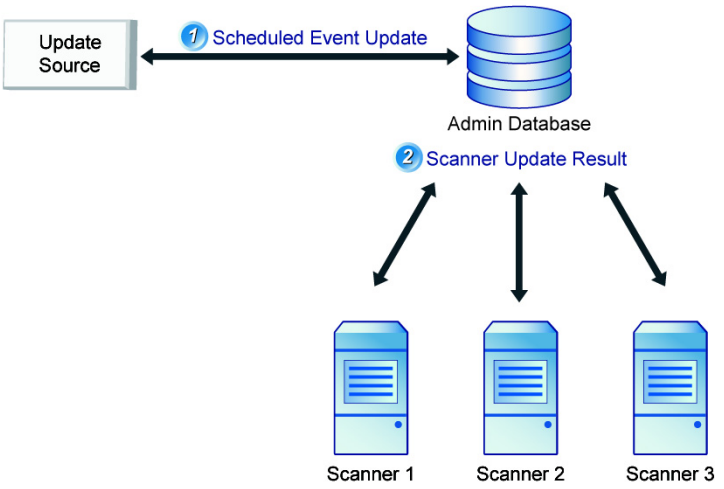


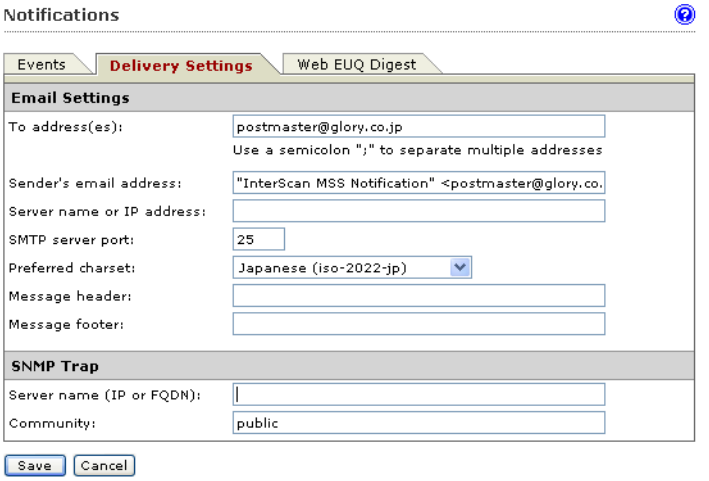
FIGURE 4-1 Scan engine and pattern file updates

Configuring Delivery Settings

The delivery settings allow you to specify the sender, recipient(s) and other settings required for delivering the notification message when certain events are triggered.

To configure the delivery settings:

1. Choose **Administration** > **Notifications** from the menu. The Events tab appears by default.
2. Click the **Delivery Settings** tab.



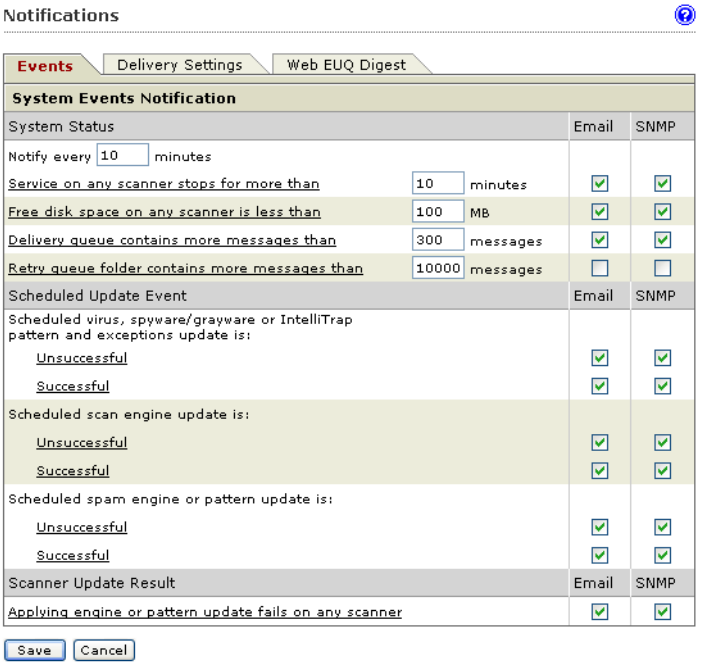
3. Provide the required information.
4. Click **Save**.

Configuring Event Criteria and Notification Message

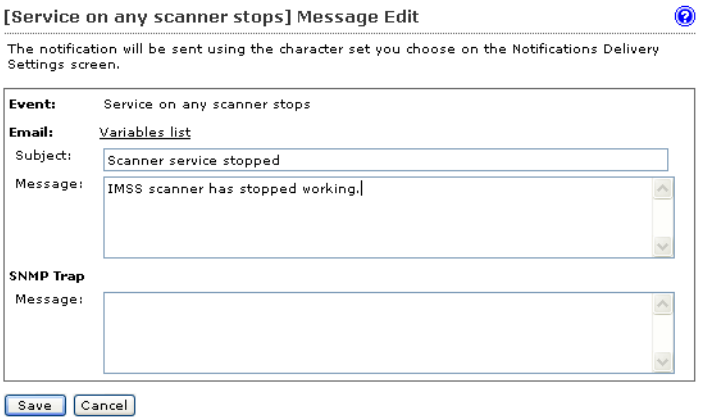
You can set the criteria under which IMSS will trigger a notification message and also customize the message content for each event.

To configure the criteria and message content:

1. Choose **Administration** > **Notifications** from the menu. The Events tab appears by default.



2. Specify the desired criteria under the System Status section.
3. Select the Email and/or SNMP check boxes according to how you would like to receive the notification.
4. To customize the message content, click on the hyperlink for the specific event. The Message Edit screen appears.



5. Type the required information.
6. Click **Save**.

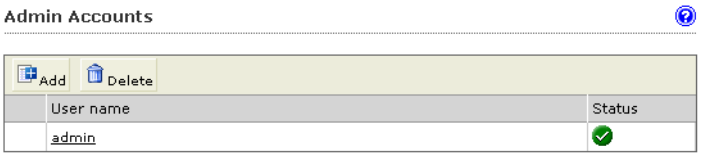
Managing Administrator Accounts

To reduce bottlenecks in administering IMSS, you can delegate administrative tasks to other staff by creating new administrator accounts and assigning the desired permissions to the various areas of the Web management console.

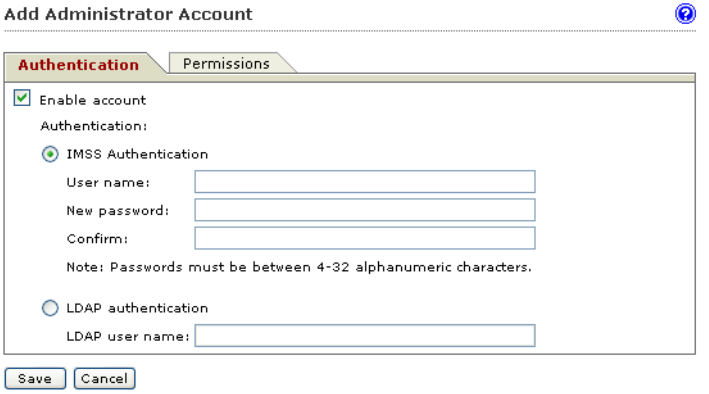
Adding Administrator Accounts

To add administrator accounts:

1. Choose **Administration** > **Admin Accounts** from the menu. The Admin Accounts screen appears.

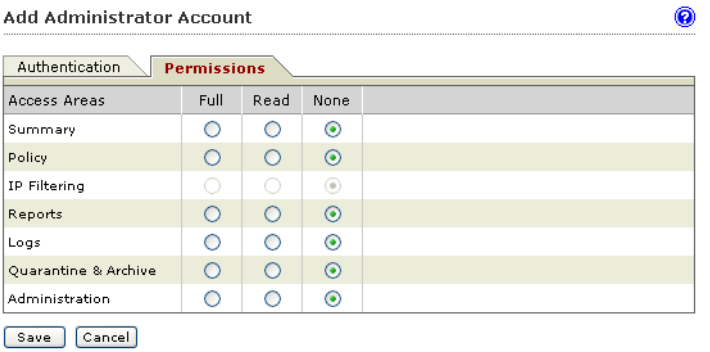


2. Click **Add**. The Add Administrator Account screen appears.



o

3. Provide the required information on the Authentication tab.
4. Click the **Permissions** tab. The Permissions screen appears.



5. Select the desired permissions to the various access areas of the Web management console.
6. Click **Save**.

Note: 1. Only the default IMSS administrator account can add new administrator accounts. Delegate administrator accounts cannot do so even if you assign full permission to the Administration area.

2. Delegate administrator accounts with full administration rights can only change their own IMSS passwords. If you forget the default administrator account password, please contact Trend Micro's technical support to reset the password.

Editing or Deleting Administrator Accounts

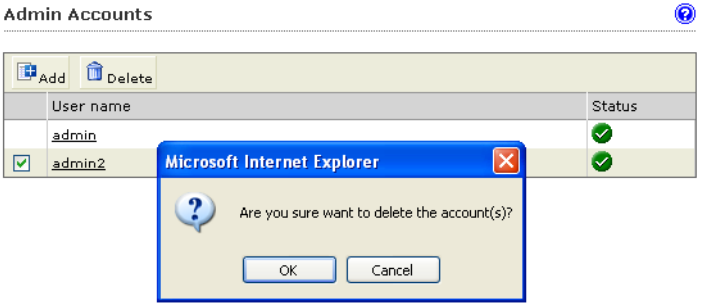
You can change or delete the permissions of a delegate whenever there is a revision of roles or other organizational changes.

To edit an administrator account:

1. Choose **Administration** > **Admin Accounts** from the menu. The Admin Accounts screen appears.
2. To edit an administrator account, click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

To delete an administrator account:

1. To delete an administrator account, select the check box next to the account to be removed.
2. Click **Delete**.
3. Click **OK** to confirm the deletion or **Cancel** to withdraw.



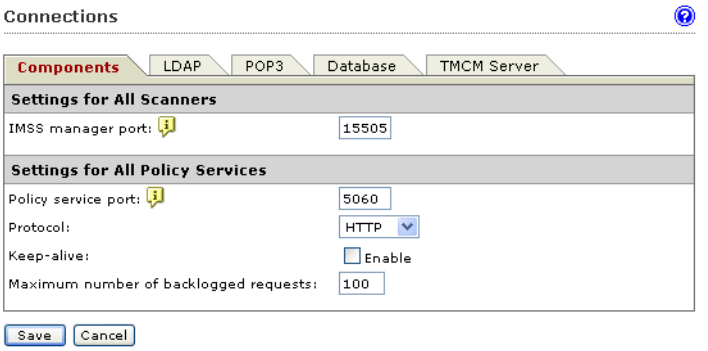
Note: You can only delete the delegate administrator account but not the default IMSS administrator account.

Configuring Scanner and Policy Connections

To enable the scanner to receive messages and also enhance the performance of rule lookups by the policy services, configure the connection settings.

To configure scanner and policy connections:

1. Choose **Administration** > **IMSS Configuration** > **Connections** from the menu. The Components tab appears by default.



2. Specify the required settings.
3. Click **Save**.

Chapter 5

Troubleshooting, FAQ, and Support

This chapter explains how to troubleshoot common IMSS issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

- *Troubleshooting* on page 5-2
- *Frequently Asked Questions* on page 5-9
- *Using the Knowledge Base* on page 5-24
- *Contacting Support* on page 5-24

Troubleshooting

Table 5-1 shows common troubleshooting issues you might encounter with the configuration and administration of IMSS. Read through the solutions below. If you have additional problems, check the Trend Micro Knowledge Base.

For troubleshooting and FAQ information pertaining to IMSS deployment, refer to the IMSS Installation Guide.

Issue	Suggested Resolution
General	
Unable to access the Web console or other components.	The target port is not in the firewall approved list. Open the ports as shown in Table 5-2 on page 5-8 in the firewall. If you are unable to access the Web console, do the following: **1.** Start the database process, `dbctl.sh`, before starting the Central Controller process, `S99ADMINUI`. **2.** If you are still unable to access the Web console, restart the Central Controller process, `S99ADMINUI`. For more details, refer to *Invoking IMSS Scripts* on page A-2.
No access to the Web console	The Web console URL is not a trusted site in Internet Explorer. Add the URL to the trusted sites.
The imssps daemon is running but refusing connections.	If the imssps daemon is running, the policy service is working. Check the connection between the policy service and scanner service and verify your LDAP settings.
Unable to activate products (Antivirus/eManager, SPS, NRS, IP Filtering) or update components	If a proxy server is on your network, verify your proxy settings. To activate NRS, IMSS needs to connect to Trend Micro. This process requires a DNS query. Therefore, if a DNS server is not available or has connection problems, activation will fail. Verify your DNS server settings. **To verify your DNS settings from the Web console:** **1.** Choose **Administration > Updates** from the menu. The Schedule tab displays by default. **2.** Click the **Source** tab. **3.** Configure the proxy settings. **4.** Click **Save**.

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
Email notifications do not display properly.	If your computer is running a non-English operating system and the notification message was not written in English, it may appear distorted. Modify the character set through the Web console. **To modify the character set:** **1.** On the Web console menu, choose **Administration > Notifications > Delivery Settings**. **2.** Next to **Preferred Charset**, select the language in which the messages will be encoded.
Cannot query message logs in IMSS.	IMSS scanner records the log with local time. To query message logs, synchronize the date/time for all machines with IMSS.
Server displays as disconnected in the Summary screen.	A managed server could become disconnected for any of the following reasons: • The scanner was removed from your network. • The IMSS manager service has stopped. • Network connection issue. Check your firewall settings for the Manager Service listening port. Click **Administration > IMSS Configuration > Connections > Components > IMSS Manager Port.**
When viewing detailed information for quarantined or archived email, attachment information is sometimes not available.	IMSS records attachment information only when the triggered rule is for an attachment. Please check the reason why IMSS quarantined the email.
IMSS does not receive email.	**1.** Check if the IMSS scanner service is running. **2.** Check if a different application is using the required port. Free up port 25.
Services are not running normally.	The database has not been started or the database was started after the IMSS services started. Restart all IMSS services.

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
End-User Quarantine Issues	
Unable to access the EUQ Web console	Do the following: **1.** Verify that you are using the correct URL and port number. To view the console from another computer on the network, go to: • Primary EUQ service—`https://<target server IP address>:8447` • Secondary EUQ service—`https://<target server IP address>:8446` **2.** Verify that the system time of each EUQ service on your network is synchronized. The first instance of the EUQ service, the primary EUQ service, runs Apache Web Server (httpd) while listening on port 8447 (HTTPS). This Web Server serves as a connection point for the EUQ clients and for load balancing for all EUQ services. If the Apache server is down, users will not be able to access EUQ console from the normal IP address: `https://{Primary EUQ Service IP address}:8447/`.

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
Users are unable to log on to EUQ Web console	Do the following: **1.** On the LDAP server, verify that the user accounts are in the correct group. Only user accounts in the approved group can access EUQ. **2.** Verify LDAP and User Quarantine Access settings through the IMSS Web console: **a.** Choose **Administration > IMSS Configuration > Connections > LDAP** from the menu. **b.** Verify all settings, especially the LDAP type and server information. If you are using Kerberos authentication, ensure that the time for all IMSS computers and the LDAP server is synchronized. **c.** Choose **Administration > User Quarantine Access** from the menu. **d.** Enable User Quarantine Access. **e.** Verify that the correct LDAP groups appear under **Selected Groups** and that the user account belongs to the selected groups. **3.** Verify that your users are using the correct log on name and password. For more information, see *Log On Name Format* on page 1-14. **4.** If the issue persists even after verifying the above settings, do the following: **a.** Choose **Logs > Settings** from the menu. **b.** Set the application log level to **Debug**. **c.** Choose **Summary** from the menu. From the **System** tab, restart the Web EUQ service. **d.** Request the user to try logging on to the EUQ Web console again. **e.** Send the log file `imssuieuq.yyyymmdd` located in `/opt/trend/imss/logs` to Trend Micro's technical support.
The EUQ Web digest does not display quarantined email information correctly	Verify that the correct character set is selected: **1.** Choose **Administration > Notifications > Delivery Settings**. **2.** Next to **Preferred charset**, choose the character set that will properly display the digest information.

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
Some quarantined email messages are not appearing on the EUQ Web console	The EUQ Web console can only access email that IMSS identifies as spam or phishing attempts. From the EUQ Web console, you cannot view quarantined email that violated other rules, such as the antivirus rule.
Cannot enable LDAP with Kerberos authentication.	Kerberos protocol requires time synchronization between the Kerberos server and IMSS. Synchronize the date/time for all computers with IMSS.
IP Filtering Issues	

FoxProxy cannot start up	There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs.
	
	To view IP Profiler logs:
	1. Go to the directory where IP Profiler is installed (by default: `/opt/trend`).
	2. Open `foxproxy.ini`.
	3. Change the value for `log_level` to **4**.
	4. Restart FoxProxy by typing the following:
	`/opt/trend/ipprofiler/script/foxproxyd restart`
	5. Open the log file by typing the following:
	`/opt/trend/ipprofiler/logs/foxproxy-general.****`

Unable to connect to FoxProxy	Verify that FoxProxy is running and that it is binding on port 25.
FoxProxy processes email messages slowly	When FoxProxy receives email, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out. **Verify that the bind service is running on the computer where FoxDNS is installed:** **1.** Type the following command: `ps -ef | grep named` **2.** Start the service if it is not running.
Unable to view connections that FoxProxy is blocking	Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSS server. Wait for at least five minutes before viewing the connection information. **To change this time value:** **1.** Open `foxproxy.ini`. **2.** Modify the value for `report_send_interval`.

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
FoxDNS is not functioning	**Verify that BIND service is running:** **1.** Type the following command: `ps –ef | grep named` **2.** Start the service if it is not running.

No IP Profiler log information exists	The following IP Profiler-related log files are in the IMSS admin database:
	• `foxmsg.****`
	• `foxnullmsg.****`
	• `foxreport.****`
	Verify that the log files exist:
	1. Go to the log directory on the where IMSS is installed (by default: `/opt/trend/imss/log/`).
	2. If the files are not present, use the following command to check if imssmgr is running:
	`ps –ef | grep imssmgr`
	3. Check if FoxProxy is running:
	`ps –ef |grep foxproxy`
	4. Verify that IP Profiler is enabled. In table 't_foxhuntersetting', the following should exist:
	`record: 'Type' = 1` and `'enable' = TRUE`

NRS does not work after being enabled from the Web console.	NRS may not work due to the following reasons: • Spam Prevention Solution (SPS) was not activated. NRS shares the same AC code with SPS. If SPS has not been activated, please activate SPS and then activate NRS. • The computer on which the scanning service is installed cannot access the Internet. MTA cannot get a response for the DNS query for AC validation. Please confirm that the computer where the scanner service is installed has access to the Internet. Please activate SPS and confirm that the computer with SPS installed can access the Internet.
The MTA settings on the **SMTP Routing** Web console screen are not being written into the Postfix configuration files	By default, the settings on the SMTP routing screen cannot be written to Postfix. Enable this function using the following steps: Go to the IMSS configuration directory (by default: `/opt/trend/imss/config`). Open the IMSS configuration file `imss.ini` Change the value for `enable_postset_thd` to yes or leave the value empty. Restart IMSS manager using the following command: `/opt/trend/imss/script/S99MANAGER restart`

TABLE 5-1. Troubleshooting issues

Issue	Suggested Resolution
IP profiler does not block IP addresses in the Blocked List.	The changes required about one (1) minute to take effect. Please wait one (1) minute.
Blocked IP address does not display in the Overview page	The Overview page displays the top 10 blocked IP addresses by type for the last 24 complete hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today. Please view the Overview page after an hour.

TABLE 5-1. Troubleshooting issues

Module	Port	Description
Admin UI	8445	Tomcat listen port (HTTPS)
Bind	53	Name-domain server
EUQ UI	8009	Tomcat AJP (load balance) port
EUQ UI	8446	Tomcat listen port
EUQ UI	8447	Load balancer
Manager	15505	SOAP server
MTA	25	SMTP
MTA	465	SSMTP (SSL)
Policy Server	5060	SOAP listen port
Scanner	10024	POP3 listen port

TABLE 5-2. Component ports

Frequently Asked Questions

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally? Can I make an exception on the settings for some Postfix instances separately?

If you want to control all the Postfix computers from the Web management console, you should enable the "**Apply settings to all scanners**" option. Choose **Administrator** > **SMTP Routing** > **SMTP** from the menu.

If you want to make an exception for some Postfix settings, you can search for the key "`detach_key_postfix`" in `imss.ini`, and add the keys that you do not want to apply from the Web management console. For example:

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory
```

How can I change my MTA settings without using the Web console?

You can modify the IMSS configuration file and add the following key.

1. Open `imss.ini`.
2. Make the following modification:

```
detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1:{Parameter2}:…::{Parameter n}
```

The parameters above will not be overwritten by any settings that you configure through the Web console. You can modify `main.cf` manually.

Note: "{Parameter1:{Parameter2}:…::{Parameter n}" means you can use one or more parameters by separating them using colons.

WARNING! *Use extreme caution when modifying the configuration file.*

IMSS Components

Can I move the Central Controller from one computer to another?

Yes. First, run the IMSS installation script to uninstall the Central Controller from the computer. Next, run the IMSS installation script and install the Central Controller on the other computer.

How can I set up and maintain the database?

The following commands can help you maintain the database:

- `pg_dump imss > YYMMDD.HHMMSS.backup`—Back up the database.
- `psql imss < YYMMDD.HHMMSS.backup`–Retrieve the latest data if errors occur.
- `vacuum`–Clean up the database on tables that are frequently accessed or on tables that have large amounts of data. Use when email traffic is low or when the device is not connected to your network.
- `vacuumfull`–Clean up the entire database when the database is not being heavily utilized or when the device is not connected to your network.
- `redirect_stderr= and log_rotate_***=` Turn on these options in `postgresql.conf` to redirect old database log entries to the system log, which is rotatable. You can name the log-file to start with a dash "-".

You can also delete some IP-Filtering and log data using SQL and modify the logs settings on the **Logs > Settings** screen.

Is IMSS policy service able to work if LDAP is down?

Yes, the policy service still works even if the LDAP server is down.

Following are three scenarios of such a situation.

- IMSS continues to work as usual.
  - If the LDAP server is active but the port of the LDAP server is inaccessible.
  - If the policy server has the non-expired cache of the LDAP user or group.
- The policy server will bypass the LDAP-related rules and continue to process other rules.
  - If the LDAP server is active, but the port of the LDAP server is inaccessible.
  - If the policy server has no valid cache for the rule.

- IMSS will spend about one minute to perform each rule query. This may slow down the message scanning and result in long mail queues.
  - If the LDAP server is down.
  - If the policy server has no valid cache for the rule.

Network Reputation Services

How do I configure Network Reputation Services (NRS) to not block certain IP addresses or domains?

Add the IP addresses / domains to the NRS approved list by doing the following:

- Log on to the Web console.
- Click **IP Filtering > Approved List**.
- Add the IP addresses or domains that you do not want blocked to the Approved List.

How do I enter the Activation Code (AC) for NRS?

You can enter the AC during installation, or you can modify it after installation.

To modify the AC, edit the Postfix configuration files located in the same computer as NRS. These files are `main.cf`, `imss_rbl_reply`, and `imss_rbl_reply.user`.

Note: The `imss_rbl_reply.user` file may not exist. If it exists, please modify it. Otherwise, you can omit it.

After installing NRS, you should see similar contents in the three configuration files as follows:

- **`main.cf`**

```
smtpd_client_restrictions = reject_rbl_client
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com,reject_rbl_
client APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com
```

- **`imss_rbl_reply`**

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450 Service
temporarily unavailable; $rbl_class [$rbl_what] blocked
using Trend Micro Network Reputation Service. Please see
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=$rbl_wha
t${rbl_reason?; $rbl_reason}
```

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 550 Service
unavailable; $rbl_class [$rbl_what] blocked using Trend
Micro RBL+. Please see
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=$rbl_wha
t${rbl_reason?; $rbl_reason}
```

- **imss_rbl_reply.user**

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com  450 error
message; $rbl_class [$rbl_what] blocked using Trend Micro
Network Reputation Service. Please see
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=$rbl_wha
t${rbl_reason?; $rbl_reason}
"APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com  450 error
message; $rbl_class [$rbl_what] blocked using Trend Micro
RBL+. Please see
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=$rbl_wha
t${rbl_reason?; $rbl_reason}
```

Replace the old AC with your new AC in these three files. The old AC shown in the above examples is APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.

Note: You do not need to type the dash '-' for the AC.

After editing the configuration files, restart Postfix using the commands:

```
# postfix stop
# postfix start
```

IP Profiler

How can I purge the FoxProxy log?

A log purge program exists in the IP Profiler installation directory (by default: `/opt/trend/ipprofiler/bin/TmFoxPurgeLog`).

The settings about log purge function are in the configuration file `foxproxy.ini`. The keys are as follows:

- `log_purge`
- `log_purge_unit`
- `log_purge_num`

Who will monitor FoxProxy's status? Who will rescue it when it shuts down?

FoxProxy is a multiple-process program. The main process only monitors child processes. If child processes are dead, the main process rescues them. But if the main process is dead, the child processes cannot be rescued.

If you are experiencing any problems with FoxProxy, verify that the main process is running.

How are DNS queries performed?

The DNS queries are performed directly by FoxProxy.

A DNS server is automatically installed on the Central Controller if the installer does not detect any existing DNS server. When you install IP Profiler, the installer will prompt you for the IP address of the Central Controller.

Why is the domain name of an IP address that was added to the blocked/approved list always N/A?

IMSS does not determine the domain name of an IP address that was added to the blocked/approved list (IMSS does resolve the IP address of an added domain name).

Why does the IP Filtering Suspicious IP screen also display the connection information of blocked IP addresses?

The **IP Filtering > Suspicious IP** screen shows all information for successful connections. Therefore, although an IP address is now in the blocked list, the previous connections for this IP address, which have not been blocked, are shown.

How does IP Profiler process email?

The IP Filter decides if the source IP address is a safe IP address. IMSS scanner service queries matched policies from the IMSS policy service. The policies are applied to the email in the required order. If a policy specifies that an email should be quarantined, deleted or delivered, then the action is taken and the remaining policies are not applied.

Can the IP Profiler use an existing BIND server?

Yes. The IP profiler requires a BIND server. When a user installs IMSS, if a BIND server is already present on the machine, the IP profiler will use this BIND server. If a BIND server is not present, then IMSS installs a new BIND server.

How can I configure BIND version 9.x to make sure IP Profiler works well?

If you did not install BIND version 9.x during installation or migration, but you want to use IP Profiler later, please do the following:

a. If an old BIND server exists, uninstall it on the target machine if the version is lower than 9.x.

b. Run the command `tar -xvf imss.tar` to get the `bind.tar` file.

c. Copy `bind.tar` to a specified folder.

d. Run the command `tar -xvf bind.tar` to extract the file.

e. Type the `cd` command to change to the bind folder. Outside the folder, you can view the following:

```
bash-2.03# pwd
/export/home/bob
bash-2.03# ls
bind bind.tar
```

f. Run the following commands:

```
chgrp -R imss bind
chown -R imss bind
chmod -R 555 bind


cp -f bind/named.conf /etc
cp -f bind/rndc.key /etc


mkdir -p /var/named
chmod 770 /var/named
```

g. If there is no named group or user, run the following command:

```
groupadd named
useradd -g named -s /bin/false -d /var/named named
```

h. Run the following commands to configure BIND server:

```
chown named:named /var/named
mkdir -p /var/run/named
chmod 770 /var/run/named
```

```
chown named:named  /var/run/named

chown named:named  /etc/named.conf
chown named:named  /etc/rndc.key
chmod 555 /etc/named.conf
chmod 555 /etc/rndc.key
```

i. Modify `foxdns.ini` as follows:

```
vi $IMSS_HOME/config/foxdns.ini
#$IMSS_HOME is /opt/trend/imss/ by default.
#modify the following item:
# /export/home/bob/bind is the folder for bind
dig_path=/export/home/bob/bind/dig
rndc_path=/export/home/bob/bind/rndc
named_pid_path=/var/run/named/named.pid
named_db_path=/var/named/ipprofiler
```

j. Type `bash-2.03# /export/home/bob/bind/named` to run the BIND server.

k. Restart S99FOXDNS at `$IMSS_HOME/`script.

When does IMSS 7.0 send an email to "`Foxhunter_proxy@domain`"?

IMSS will send an email to "`Foxhunter_proxy@domain`" under the following three conditions:

- When FoxProxy receives an "Incomplete" message.
- When FoxProxy receives a "Null" message.
- When FoxProxy rejects a connection, it will send a statistics mail every 5 minutes. You can configure the time interval by modifying the `report_send_interval` (unit in seconds) setting in `foxproxy.ini`.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Technically, LDAP service is not a must-have. The DHA rule of IMSS 7.0 relies on the result returned from Postfix, which in turn passes the result to FoxProxy, a sub-module of IP Profiler, for analysis. The LDAP server is just one of the many means by which Postfix checks for the existence of a recipient's mailbox.

Quarantine and Archive

What special characters can be used for searching?

Use an asterisk (*) as a wildcard and a semicolon (;) to separate recipients or attachments.

Why is there a quarantined message without message-id when the user views the message detail?

IMSS will reprocess notification mails for security reason. Therefore, if a notification mail was quarantined due to the policy settings, then this notification mail generated by IMSS would not have a message-id.

If you do not want IMSS to scan the notification mails, you can disable notification mail scanning as follows:

a. Modify the following setting in the [general-notification] section of the `imss.ini`:

`NotificationSkipScan=1`

b. Restart IMSS daemon by typing the command `$IMSS_Home/script/S99IMSS restart`.

WARNING! *Trend Micro does not recommend that you disable the scanning for notification mails as there is the risk of a security leak caused by the policy settings.*

End-User Quarantine

If I am using Kerberos, why are users unable to log on to the EUQ console with a short name: "domain\user_name"?

Kerberos servers cannot accept user names in the format: `Domain\user_name`. Kerberos requires the format `user_name@domain.xxx`

If I installed Exchange Server, and have set multiple mail addresses for each user, how do I enable EUQ to check multiple mail addresses for one user?

If you installed one Exchange Server together with the Active Directory, you can do the following:

a. Open the table `tb_global_setting` in IMSS administrator database and replace the value of `LDAP-->mail_attr` from "mail" to "proxyAddresses".

b. Restart all IMSS services.

How do I send a Chinese EUQ digest?

Do the following:

a. In the Web console, click **Administration > Notifications >Web EUQ Digest**.

The Web EUQ Digest screen appears. Type the EUQ subject or content in Chinese.

b. Click **Administration > Notifications > Delivery Settings**.

The Delivery Settings screen appears. Select Chinese as the Preferred charset.

How can I speed up my LDAP access if the LDAP server is Active Directory?

There are two methods to speed up your access. The method you use depends on the port number you can use: port 389 or port 3268.

Active Directory uses 3268 for the Global Catalog. LDAP queries that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

Tip: Trend Micro recommends using port 3268 for LDAP queries.

Active Directory uses port 389 for LDAP query. If one item cannot be queried in one domain controller, it uses the LDAP referral mechanism to query another domain controller. Use port 389 if your company has only one domain or if port 3268 is unavailable.

To use port 3268 for LDAP queries:

a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.

b. Click the **LDAP** tab.

c. Configure the LDAP listening port as 3268.

To use port 389 for LDAP queries:

a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.

b. Click the **LDAP** tab.

c. Configure the LDAP listening port as 389.

d. Add the following key into the `imss.ini` file, which is at `$IMSS_HOME\config`.

```
[LDAP-Setting]
DisableAutoChaseReference=yes
```

e. Restart all IMSS services.

What user logon name formats does IMSS support for Active Directory?

Active Directory supports the following logon name formats:

- Example 1: `bob@imsstest.com`

Note: The logon name is not email address (though it appears as one).

- Example 2 (pre-Windows 2000): `IMSSTEST\bob`

Note: The pre-Windows 2000 format is not supported by Kerberos authentication.

Spam Protection Service

How is the spam catch rate determined?

Specify a threshold value between 3.0 and 10.0 for IMSS classification of an email message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).

ActiveUpdate

How do I roll back a pattern file?

Click the **Rollback** button on the Summary page.

Others

What do I have to do to use SMTP over Transport Layer Security (TLS)?

Upload the certificate for TLS and enable it on the **Administration > IMSS Configuration > SMTP Routing** screen.

IMSS 7.0 uses the Postfix TLS function. All settings are written to the configuration file `main.cf`. For more information, see:

`http://www.postfix.org/TLS_README.html`

Can the database server be referenced by hostname?

Yes.You can specify the "`IP\Instance`" or "`Hostname\Instance`".

Can the server IP address be changed?

Yes.

To change the server IP address:

a. Stop all IMSS services by running the `$IMSS_Home/script/imssstop.sh stop` command or stop the services individually with the following scripts:

```
S99IMSS stop
S99Policy stop
S99EUQ stop
S99CMAGENT stop
S99ADMINUI stop
S99FOXDNS stop
S99MONITOR stop
S99MANAGER stop
dbctl.sh stop
```

Refer to Appendix B for details of each script.

b. Change the server IP address.

c. Change the IP address in `ODBC.ini` and `EUQ.ini` in the IMSS configuration folder.

d. Change the database URL and user name/password in `%IMSS_HOME%\ui\adminUI\webapps\ROOT\WEB-INF\struts-config-common.xml`

e. Change the following database data:

- `tb_component_list`: Specify the computer name and all scanner IP addresses.
- `tb_euq_db_info`: Specify the EUQ database computer settings.
- `tb_global_setting`: In section [cmagent] name [ConfigUrl], change the Web console URL.

f. Restart all IMSS services with the scripts located in `$IMSS_Home/script`.

Begin with the following scripts:

```
dbctl.sh start
S99MANAGER start
```

The remaining services can be restarted in any order:

```
S99IMSS start
S99Policy start
S99EUQ start
S99CMAGENT start
S99ADMINUI start
S99FOXDNS start
S99MONITOR start
```

How does IMSS process a partial email?

IMSS rejects partial email as a malformed message if `BypassMessagePartial=no` in the `imss.ini` file (default setting).

If the key is set to `yes`, IMSS will bypass the partial mails. Trend Micro does not recommend changing the item "BypassMessagePartial" to `yes` as this may cause virus leak.

What file format can IMSS import when configuring policy settings?

IMSS can only import .txt file containing only one item per line. Following are examples of how you can import a text file from the Web management console:

a. When specifying the attachment to be scanned

- Click **Policy** > **Policy List** from the menu.

- Click on the link of an existing rule to edit a rule.
- Click on the **And scanning conditions match** link.
- Click the **Name or extension** link under the Attachment section.
- Select the check box next to **Attachment named**.
- Click **Import**. The imported file should be a text file containing one file name or extension per line.

b. When configuring the spam detection settings

- Click **Policy** > **Policy List** from the menu.
- Click on the link of an existing rule to edit a rule.
- Click on the **And scanning conditions match** link.
- Click the **Spam detection settings** link.
- Select the check box next to **Approved sender list** or **Blocked sender list**.
- Click **Import**. The imported file should be a text file containing one email address per line.

Why can't newly created administrator accounts access the User Quarantine Access, Admin Accounts and Product License pages?

Only the default IMSS admin account has the permission to access the User Quarantine Access, Admin Accounts and Product License pages. Delegated admin accounts cannot access these pages.

Why are changes to the IMSS configuration settings not effective immediately?

There is a lapse between the time you modify the configuration settings from the Web management console and the time modifications are actually updated on the IMSS server.

Policy settings will be reloaded in no longer than three (3) minutes. If you want the settings to load faster, please modify the `policy_server=>dbChangePollIntervalInSecs` setting in the `tb_global_setting` table of the IMSS administrator database as desired.

For other general settings, imssmgr will take no longer than one (1) minute to reload the new settings modified from the Web management console.

Trend Micro recommends that you do not send mail to IMSS immediately after modifying the configuration settings from the Web management console.

Is there any limit on the maximum number of the following items?

- **Senders and recipients for each rule**
- **Mail addresses in one address group**
- **Approved/Block Senders for SPS rule**

  Technically, there is one limitation on the total size of each rule, which is 640kb. The total size includes the rule route (senders/recipients), rule filter (scanning condition), and rule action. Assuming that each email address/LDAP account consists of 20 characters, IMSS can support at least 10,000 senders/recipients for the rule route.

  The maximum number of mail addresses for one address group is 10,000.

  The maximum number of Approved/Block Senders for SPS rule is 5000.

How can I modify the log paths?

If you want to modify some log paths, please locate the following keys in `imss.ini` and change the default settings as desired.

```
[general]
sys_log_path=/opt/trend/imss/log
event_log_path=/opt/trend/imss/log
policy_evt_log_path = /opt/trend/imss/log
[policy_server]
log_path = /opt/trend/imss/log
…
[logs]
log_path=/opt/trend/ipprofiler/logs
```

Can IMSS 7.0 configure its own relay restrictions if a third-party upstream server is not installed?

No. IMSS 7.0 cannot configure its own relay restrictions as it does not have its own MTA on the Unix platform. You can only configure relay restrictions using a third-party MTA.

How can I modify the Access Control List (ACL) for the IMSS scanner?

You can modify the following settings in `imss.ini`.

- Add the target IP address to the parameter `smtp_allow_client_ip`.
- Alternatively, disable ACL check by setting `open_to_all_connections=yes`.

- To ensure that other computers are able to connect to the scanner, insert the target IP addresses in the parameter `proxy_smtp_server_ip`.

For more details, please refer to the comments in `imss.ini`.

Mails from some senders are always received as attachments. The mail body is also replaced by the disclaimer or stamp. Why is that so?

When the charset of the stamp is different from the charset of the mail content, IMSS will encounter issues inserting the stamp into the mail body after scanning the mail. In this situation, IMSS will create a new mail, insert the stamp into the mail body and attach the original message. The mail content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as "from", "to", or "subject" when creating rules with content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use "`^(\s)*$`" (without the quotation marks). The expression "`^(\s)*$`" (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a mail's "**from**" header is blank, you can edit a rule's scanning condition as follows:

a. On the Web management console, click **Policy**>**Policy List**.

b. Click the link for an existing rule to edit the rule.

c. Click **And scanning conditions match**.

d. Click **Header keyword expressions** under the **Content** section.

e. Click **Add** to create a new keyword expression.

f. Add the content as "`^(\s)*$`" (without the quotation marks).

Using the Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

`http://esupport.trendmicro.com`

The contents of the Knowledge Base are updated continuously, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Contacting Support

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users. Get a list of the worldwide support offices:

`http://www.trendmicro.com/support`

Get the latest Trend Micro product documentation:

`http://www.trendmicro.com/download`

In the United States, you can reach the Trend Micro representatives via phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.
Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: www.trendmicro.com
Email address: support@trendmicro.com

Appendix A

IMSS Scripts

This appendix provides you with a list of IMSS scripts and their respective parameters that you can invoke from the command line.

Topics include:

- *Invoking IMSS Scripts* on page A-2

Invoking IMSS Scripts

IMSS scripts provide a convenient and alternative means of performing administrative tasks from the command line.

See Table A-1 for a list of the scripts, their respective parameters and the functions they perform.

Note: All scripts listed in the table are located in `/$IMSS_Home/imss/script`, except `foxproxyd`, which is located in `/$IMSS_Home/ipprofiler/script`.

Scripts	Parameters	Descriptions
foxproxyd	start / stop / restart	IP Profiler service
dbctl.sh	start / stop / restart	Postgres database service
imsstop.sh		Forces all IMSS services to stop.
postfixctl.sh	start / stop / reload / restart	Postfix daemon
regippro.sh	reg / unreg	Register or unregister IP Profiler to or from the admin database.
S99ADMINUI	start / stop / restart	Central Controller
S99CLEANEUQ		Removes expired quarantined data from the EUQ and admin databases as configured under the **Administration** > **User Quarantine Access** area of the Web management console.
S99CLEANEXPIRE		Removes expired quarantined and archived data from the EUQ and admin databases as configured under the **Quarantine & Archive** > **Settings** area of the Web management console.
S99CMAGENT	start / stop / restart	CMAgent service
S99DIGEST		Sends the EUQ digest message
S99EUQ	start / stop / restart	EUQ service

TABLE A-1. IMSS scripts

Scripts	Parameters	Descriptions
S99FOXDNS	start / stop / restart	Foxdns service
S99IMSS	start / stop / restart	IMSS scanner service
S99MANAGER	start / stop / restart	Manager service
S99MONITOR	start / stop / restart	Manager monitor service
S99POLICY	start / stop / restart	Policy service
S99REPORT	[option] start / stop / restart [option]: • **-s**—generates centralized reports (covers all one-time and scheduled reports configured on the Web management console) • **-h**—generates hourly individual traffic data • **-t**—generates hourly traffic data • **-d**—performs database log maintenance	Used by S99SCHEDULED to generate related reports. **Note:** Do not run this script on its own.
S99UPDATE	start / stop	Used by S99SCHEDULED to run the scheduled update. **Note:** Do not run this script on its own.
S99SCHEDULED		Starts the scheduled task.
forceUpdate.sh	DBDSN username password	Notifies the policy server to reload the policy settings
euqtrans		Transfers EUQ database data

TABLE A-1. IMSS scripts

Appendix B

Default Directory Locations

This appendix provides information on the default directory locations that IMSS uses for mail processing.

Topics include:

- *Default Mail Queues* on page B-2
- *eManager, Virus and Program Logs* on page B-3
- *Temporary Folder* on page B-3
- *Notification Pickup Folder* on page B-3

Default Mail Queues

Table B-1 shows the various mail directories that store the mail messages managed by IMSS.

Queues for Regular Mails	Queues for Large Mails	Descriptions
queue_malform=/opt/trend/imss/queue/malform		Stores malformed messages.
queue_archive=/opt/trend/imss/queue/archive		Stores archived messages.
queue_quarantine = /opt/trend/imss/queue/quarantine		Stores quarantined messages.
queue_notify=/opt/trend/imss/queue/notify	queue_notify_big=/opt/trend/imss/queue/notifybig	Stores notification messages.
queue_postpone=/opt/trend/imss/queue/postpone	queue_postpone_big=/opt/trend/imss/queue/postponebig	Stores postponed messages.
queue_deliver=/opt/trend/imss/queue/deliver	queue_deliver_big=/opt/trend/imss/queue/deliverbig	Stores messages for final delivery.
queue_reprocess=/opt/trend/imss/queue/reprocess	queue_reprocess_big=/opt/trend/imss/queue/reprocessbig	Stores messages pending reprocessing.
queue_handoff=/opt/trend/imss/queue/handoff	queue_handoff_big=/opt/trend/imss/queue/handoffbig	Stores messages pending handoff.
queue_undeliverable=/opt/trend/imss/queue/undeliverable		Stores undeliverable messages.
queue_unnotify=/opt/trend/imss/queue/unnotify		Stores undeliverable notification messages.

TABLE B-1. Default IMSS Mail Locations

eManager, Virus and Program Logs

Many modules in IMSS write log information for troubleshooting purposes to the following folder:

```
/opt/trend/imss/log
```

Temporary Folder

IMSS stores all application-generated temporary files in the temporary folder:

```
/opt/trend/imss/temp/
```

Note: This directory is not configurable.

Notification Pickup Folder

IMSS stores all notification messages and picks them up from the following folders, then delivers them to a specified SMTP notification server:

```
/opt/trend/imss/queue/notify/ and
/opt/trend/imss/queue/notifybig
```

To configure the SMTP notification server:

Choose **Administration** > **Notifications** > **Delivery Settings** from the menu.

Note: The queue_notify_big queue is for large mail messages.

Index

A

address groups
  examples of 2-25
AJP 5-8
APOP 2-21
audience vi

B

basic configuration 1-4

C

commands A-2
connections 2-14
contact support 5-24

D

Documentation vi
domain-based delivery 2-17

E

EUQ
  Web console 1-14

F

FAQ
  EUQ 5-16
  IMSS components 5-9
  IP Profiler 5-12
  postfix 5-9
  TLS 5-19
filters
  examples of 2-25

I

Install 1-1, 2-1, 3-1, 4-1
installing
  using SSL 1-3

K

Knowledge Base 5-24

M

MTA
  with NRS 2-3

N

NRS
  Activation Code 2-2
  Administration Console 2-4
  MTA settings 2-3
  using 2-2

O

Online Help vi

P

password
  IMSS Web console default 1-2
permitted senders 2-17
POP3 listen port 5-8

R

Readme File vi

S

scanning conditions 2-36
setup wizard 1-4
SMTP routing 2-14
SOAP server 5-8
Spam Prevention Solution (SPS)
  Activation Code 2-2
SSL certificate 1-3
support 5-24

T

transport layer 2-15
Trend Micro Knowledge Base 5-24
troubleshooting 5-2
  activating products 5-2

email notifications 5-3
EUQ quarantined messages 5-6
EUQ Web console access 5-5
EUQ Web digest 5-5
imssps daemon 5-2
IP Filtering 5-6

U

user name
IMSS Web console default 1-2

W

Web console 1-2
wizard 1-4